ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

CyberSight25

Problem 4

Achieving 100% with CMDB

LINEO RACOCO

Hyb Arloesedd Seiber
Cyber Innovation Hub

REGISTRATION FORM

ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

Alliances

www.alliances.global

ALLIANCES X CYBER INNOVATION HUB

WHY?

As the Alliances have access to a breadth of professionals are up to speed on the reality of impacting senior Information and Cybersecurity Roles.

The Cyber Innovation Hub, held out of Cardiff University has partnered with the Alliances to elaborate on it's previous and utilise the community and their knowledge around its initiatives. We will be focusing on:

- Introducing Cyber Innovation Hub – a game changer in spinning science into cyber solutions...
- How is Cyber Innovation Hub solving the cyber problems of today and tomorrow?
- CyberSight25 – defining the solutions of tomorrow
- The Ask from the community and what do they get out of it.

WHAT IS CIH?

Introducing Cyber Innovation Hub – a game changer in spinning science into cyber solutions...

Cyber Innovation Hub is spun out of Cardiff University's Centre for Cyber Security Research (CCSR). CCSR has been operating for a decade and takes a challenge-focussed approach to applied cyber research, having developed strong industry partnerships and seen research translated into commercial processes. To date, spin out companies from this research have been limited. Largely due to a lack of capacity in the academic team to explore markets and develop commercial cases – but equally due to a lack of commercial and business skills within the team to actually take a commercial venture to market.

How is Cyber Innovation Hub solving the cyber problems of today and tomorrow?

CIH is solving this blocker by match-making the academic solution creators with entrepreneurs in the Alacrity Foundation's incubation programme. Alacrity hire business leads and train them in an intensive 12 month programme. The entrepreneurs on the programme are business-focussed, and learn how to identify commercial opportunities, understand customer needs, develop business plans, and take a solution to market. The CIH programme will wrap a team on the Alacrity programme around academic solution creators, and provide them with support and services to scale quickly. We believe this is a globally unique programme – pulling cutting edge scientific intellectual property into commercial ventures to solve the World's most pressing cyber security problems.The Ask from the community and what do they get out of it.

WHAT IS CYBERSIGHT25?

CyberSight25 – defining the solutions of tomorrow

CIH is seeking thought leadership in defining the cyber security problems of today and tomorrow, and is partnering with the Alliances team to run the CyberSight25 campaign. By 2025, we aim to have 25 well defined cyber problems, articulated by 25 of the World's leading cyber experts. This includes CISOs, CIOs, and anyone else who is living and breathing a cyber problem that they just can't find the right solution for – despite all the marketing hype!

The Ask?

There is some time required for input to CyberSight25 – so we're only seeking those who are most committed to the advancement of cyber solutions and mentoring future business founders to support the sector. The ask is as follows:

- An initial meeting to discuss the problem you would like to bring to the campaign
- Some of your time spent articulating what a "good solution" would look like – an outline to guide the CIH in developing a solution
- A 30 minute mentoring call with the CIH entrepreneurs every 2 weeks over a 6 month period during ideation and wireframing of the solution

What do you get out of it?

This is a clarion call for your knowledge and passion for the sector, to shape the solutions of tomorrow, and to mentor the next generation of cyber entrepreneurs!

TRANSCRIPT

Leigh -
Welcome everyone to a partnered podcast with Cyber Site 25, which is part of the Cyber Innovation Hub, which is part of Cardiff University. My name is Lee Thomas. I'm the founder and director of the alliances, the regional director of South Africa.
I'm with a wonderful community member from our South Africa community in Lineo Rocho, could you kindly introduce yourself and give a bit of context in terms of your industry impact, and what you're about?

Lineo -
Great. Thank you very much Leigh, I really am. I'm really glad to be part of this platform. And thank you again for the intro.
So obviously my name is Lineo. I am a cyber professional, been in the industry for just over 17 years and currently I hold the position of a group CISO in a global FMCG organisation.
Which is also, I'm a first time CISO, so it's interesting to see the world of cyber from a different lens.
I've obviously had to put on the executive leadership head business hat. So it's quite interesting. It's quite humbling, but quite an exciting journey to actually be able to articulate the cyber risk in a language that business can actually understand.

Leigh -
So in terms of a bit of an overview from an objective standpoint, when it comes to cyber security and what could you provide us with a bit of an overview of how you're seeing things at the moment?

Lineo -
Look, not so long Ago I was actually looking at the Microsoft 2023 digital Defence report.
In that particular report, they say that on a literally every second they block about 4000 identity attacks. This is in a second right and they they facing I think just over 7.3000 or so password attacks you know. Individual password attacks. So what that tells me is that's a big attack vector at this point in time, right? All the adversaries, the bad guys, they trying to Access our systems so I think it's really a a big pain point for most seasonals, certainly for most organisations and I see majority of organisation in the industry vertical that I'm in, they are actually looking and and and actually investing in in zero trust capabilities.
Needless to say, they sell big buzz in a big.
Move, you know, into emerging techs, more specifically, generative AI, and that's now is adding to our grey hair because now business wants this thing because you know it promises revenue and you know revenue and and you Know competitive edge, etc. But then there's also, you know, risks That it could potentially bring, I think in the past 3-4 months or so, Gen AI has been quite a pain point, quite an A topic of interest. So I think as the cyber leaders, we really need to See how we enable businesses to still Dr margins revenue without compromising security and introducing business risk. So that's one of the Things that are coming to mind, I think one of the things obviously Needless to say is as much as we are technology leaders as much as we are out there to deploy this technological or technical controls, we still need to think like a business.
And we, our job and our mandate is to ensure that we assist business to operate, but do so securely. So without being, you know, traditional blockers of things, we allow responsible use and you know, obviously balancing security and convenience, right. So that's that's really, yeah.
I mean, the cloud was also a big buzz, big data, all of these wonderful things. But I think it's the challenge is how do we know of this concept? How do we pre empt you know what the Imagine tech is going to look like and how do we not just focus on today but plan for tomorrow in our Solutioning and also allow For growth and another thing, as you're speaking that comes to mind is Compliant business leaders, essentially we supporting business, right? We need to be very mindful of what are the regulatory requirements from a data privacy perspective. I mean depending on the industry that you're working in, if it's highly regulated, there's you know the likes of PCI, if you're in a banking environment You know these these sevens of, for instance, in my organisation, for instance, we need to comply to socks, so there's there's quite vast regulatory requirements that

TRANSCRIPT

we need to obviously have in mind as we're implementing our technical controls to make sure that they can actually Help us and they can actually Put us in a better place to actually be able to comply with this regulator.

Leigh -
Could you specifically, highlight the cyber security challenge or security challenge that you are facing at the moment or the industry is?

Lineo -
Certainly I want to speak very generically in terms of what I've seen happening in the industry, both in my past and possibly in in, in some cases my current space look we I mentioned earlier, we are technologically driven, right? I can't manage cyber risk without deployment of technology. Right. The biggest challenge that I'm seeing is how do we measure if this technological controls are actually effective in managing risk, right? What I've seen, you know, the KPI's that are put on, you know, various forecasts, it's it's, you know, things like coverage. Ohh great and Well, we've got I don't know 100% coverage on the EDR platform et cetera, but how do you measure if that is actually, you know effective it's I think it's the question of control presence versus you know control efficacy.
So so I want to also make a few examples so that I can sort of bring this closer to home I mentioned earlier. Identity attacks are on the rise. Majority of organisations are leveraging Active Directory either on Prem or Azure depending on obviously their different dynamics of different organisations.
But we find that the very same mechanism to securely connect or allow connections or or or authentications or authorizations into systems. If it's not securely configured, it's a problem, right? It's almost like locking your door and leaving the window open, right? So what? The biggest challenge is in that space that I would really like the listeners to maybe think about a potential solution to this. How do we ensure that our Active Directory or equivalent is actually configured securely? How do we, you know, there's, for instance, your GPO policy, right. Your group policies. I mean, if you configure group policy 80s is finicky in a sense that you can actually configure two different policies and one overrides the other, but there's no mechanism to actually detect that you have conflicting, potentially conflicting policies, right? So that defies it defies the attempt of you securing your environment because then one
Policy may supersede the other. There is nothing, at least from the little knowledge I may have, that I've seen that effectively, you know, analyses Active Directory. From that perspective, I'll make another example of multi factor authentication, another mechanism you know from embedded security or what do you call it? Multi layer security principle?
If multi factor is enabled, tick all great and well, but how do we know if you know that we have the entire estate that has multi factor enabled and is actually switched on effectively right, right. That's another area that I can think of as weak.
Right. We have had a great password policy that says I don't know 20 characters of Alphanumeric. I think that's what the majority of organisations are doing. I can help they. They even now go as far as past what past phrases right? They have a long, big sentence, you know, a couple of letters and numbers. Great. I can have a long password.
What I love pizza on Fridays long enough.
But guess what? It's key text because it's easily guessable. So do we. You know, it will be great to have some technology to actually Check even if AD will say tick you made the password policy but is that password policy not weak? So these are the kind of very quick wins very you know small things but that actually have a big risk organisation if not done correctly it will be great to have a technology that just tests the Efficacy of our controls From a single pane of glass, I can go deep as you know, for an ability management.
You know, the majority of these technologies are agent or client based. You deploy a client. The assumption is if you have coverage and the clients or agents are being deployed in the entire estate, how do we know if the clients are actually healthy, right without having to log on five different management consoles which is the case.

TRANSCRIPT

More of organisations, so it will be really great to have one Solution that actually gets data from all of these security controls. Check if they are effective. If you know if it's an agent, is it healthy, you know and stuff. So it's it's. That's it. It would be really an amazing, innovative way to just, you know, the click of a button, test your posture based on the effectiveness of your security controls.

Leigh -
Could you explain how those issues potentially come about and what potential consequences will come from it if it's not if not developed?

Lineo -
Yes, I can make an example about Active Directory because I think most people are familiar with that technology. Most organisations are leveraging it so. So I mean with the move to the cloud, you still find a bit of remnants of on Prem Active Directory instances right also?
Legacy and all of that stuff, we still find, you know, hybrid environments. So what I've seen is sometimes you would have You know, superseding policies, for instance, that are configured in AD cloud version of AD versus the on Prem and one will override the other make going to make an example about let's say password expiry policy. If you've got a password expiry policy on on Prem good it great but it's not affected because there's an overriding policy on AD.
Then it means you could essentially have people with expired passwords that are still accessing your environment, potentially terminated employees because there's no mechanism to actually lock that door so somebody still has entry, because guess what, they have the key and that key is not changed and that key remains static, which is your password not expiring essentially. So I think for me that's that risk. I mean the fact that access and identity attacks are on the rise and there are the majority of risks based on that report, at least from Microsoft that I was looking at not so Long ago. It means then we define, You know the the security controls by us. Leaving that door open essentially. So that's some of the risks that I can think about. You know, an adversary can actually compromise an account and actually get in because that account, you know, even if it expired, is still essentially active. So I think that's just one of the quick close to home examples that I can share.

Apart from a potential compromise, right? I mean, that's that, the core of what we do is protecting the organisations from unauthorised access, because anybody who wants to force entry And and gain unauthorised access. Obviously they don't have the best of motives, right? So it obviously will be unauthorised access. The question is what's the motive? If the motive is to you steal data, Drop a malicious payload and do funny, finicky things you know, so it could be a breach. It could be a a data compromise. And I mean the ripple effect can can be adverse depending on who has the you know the gotten hold of that access and what the intention to get to gain access.I mean, apart from reputational damage, I mean there could be potential financial risk. You know, they could, you know, they there could be potential compromise of personal data violation to privacy laws, potential fines. And it just goes on and on. So the big the risk is massive, Depending on obviously the intention of the, the the bad guy that has gotten hold of.

TRANSCRIPT

Leigh -
Is their solutions aiming towards this or is this a true gap within the industry that you've seen and have you tried anything to combat this challenge? If so, could you share why this hasnt worked?

Lineo -
I'm either searching In the wrong places, Or not a lot of vendors are playing in that space. I found a specific tool, it seems promising but I think there's a gap because the focus is on Different types of telemetry so it will then integrate with the likes of a vulnerability management technology. But it doesn't go as far as to query and actually do you know those ad use cases that are mentioned. It doesn't claim that space.
It would be ideal to have a tool that actually would even solve for something like a CMDB, like an, you know, asset inventory because you know it would be great to just scan the entire estate and say, OK, this particular endpoint has this many controls deployed. It's lacking this and this because that You can actually test your coverage if you know, but not only that, but also the control presence, but also the effectiveness of the control. So I think that it will be ideal to have a tool that actually solves for that.
Because I think their tools are running independently, and obviously they're focused on different things. But imagine a favourite tool that actually consolidates and just all of that data to give you a proper dashboard at a click of a button that gives you your estate in, you know, from an inventory perspective, from the control presence perspective, the coverage as well as.

Leigh -
Would this solution work with in your environment and do you also think it would work in most environments?

Lineo-
So I think this will work for most environments because I've been talking quite generically. You know, if you find this problem in a banking environment in a manufacturing environment, in a firm, big, small organisations, they face a similar problem. I mean I've, I've, I've worked in cyber for 16 years or so.
Just under 17 years, I have never worked for a company that has an 100% accurate CMDB.
So why aren't we able as organisations and as technology leaders, to solve the CMDB issue?
Because if you don't know about it, guess what? It's a risk and you won't be able to protect it.
So why? What is it? What's failing? Why aren't we able to solve it? Let alone rope devices that just get plugged in, that's a different story altogether. But the authorised devices that are in the environment company issued endpoints, how come we haven't mastered? The asset inventory, CMDB Concept. So I think it would be good to find a tool that can actually marry all of this capabilities together to try to solve not for one thing, but majority of pain points at ago.

TRANSCRIPT

Leigh -
In terms of the collaboration with the Cyber Innovation Hub, how would you see that working to develop a solution to this challenge?

Lineo -
Look, I I would assume they would obviously have to do a deep dive exactly into a particular use case. And also I just unpack, understand because there's different technologies for different Purposes. I mean, if vulnerability management is a vast of you know applications.
How do these different solutions work together or talk to one another? Because I'm assuming I'm not very technical, but I'm assuming there needs to be some API integrations and all of those Entities, so they need to understand the technicalities you know of, of getting that solution in. What? What does it mean from an integration perspective? It's different data sets from different data sources. How will their tool translate?
Or read or make sense of that data that is coming from various places potentially in different formats, so they need to, I guess, interact with, you know, and technical. Somebody in SME. Look, I have a team of brilliant minds that are very keen to be also participating in involving themselves in this kind of initiatives.
I would by all means, you know, get a sort of a think tank together and hopefully it will be great. And then just, you know, just throw ideas there and understand exactly what this mean. Because surely it's easier said than done, but I'm sure it's possible. So yeah, I think it's it's a workshopping, A brainstorming session of thoughts, just to gather the thoughts, and it will articulate what are the pain points. Why is this happening, you know, and and you know the why, I guess and then we can then get to the how And the what tangible output that we actually would make sense for particular?

Leigh -
What's the metrics or how would you go about measuring the success or the impact of the solution?

Lineo -
if I must give you a diplomatic business answer, it will be 0 audit findings because that's what business intends right? Always say I'm more scared than I'm more scared of attackers than I am of auditors. But guess what? Auditors have the loudest voice and business tends to really believe them and auditors are picking up this control deficiency issues, that's that's what they're raising, right? You know, so imagine if you had a tool that actually proactively informs you of where your deficiency areas are from a control perspective and you actually have an opportunity to remediate when audit comes, literally they're going to come in.
And and they won't find much, because then you know that You know solutions or your technical controls are effective. So I think that that is the ultimate and and the biggest.

TRANSCRIPT

Leigh -
Any particular KPIs that you can list, possibly outside of or within the audit that they would use to measure the success?

Lineo -
Look, I mean, from the examples I've given you, obviously.

I'm sure the Use cases are many, but I mean for instance, Let's say weak passwords I mean that could be a KPI. I mean a percentage of weak passwords in Their state, you know.
Relative to the number of users, if you have, if you're working for a large organisation, Users 15,000 users. Surely even 1% of that. With weak passwords, you know it opens you to risk. Yeah, so that should be one of those. I mean, I mean, obviously there's technical metrics, there's, you know, quantitative qualitative I think collaboratively based on what the outcome is or the end result. These we can then define how then can we measure if this is answering or solving for the business Area that we're trying to solve, yeah.

Leigh -
Would you consider procuring something like this solution?

Lineo -
Definitely. Most definitely, most definitely. I think it will solve A big pain point for most of you know cyber leaders across, at least in Africa, which is a market I'm familiar with. Definitely, I think that that has a big potential to penetrate the market and actually add value because I haven't seen a lot of technologies that are playing in that space. You know they may have better pieces of that. But I'm not very convinced that there is one solution that can do that. What we just talked about. Yeah, as I said, I may Be searching in the wrong places.

Leigh -
Thank you so much for your time today Lineo, its been a pleasure.

Lineo -
Thank you Leigh

KEY POINTS

Introduction:

- Lineo is a cyber professional with over 17 years of experience.
- Currently holds the position of a Group CISO in a global FMCG organization.
- Emphasizes the shift to an executive leadership role, wearing a business hat to articulate cyber risks in a language that the business can understand.

Current Cybersecurity Landscape:

- Refers to the Microsoft 2023 Digital Defense report.
- Highlights the prevalence of identity attacks and password attacks every second.
- Observes a growing interest in zero trust capabilities and a trend towards investing in emerging technologies like generative AI.

Challenges in Cybersecurity:

- Identifies the challenge of measuring the effectiveness of technological controls in managing cyber risks.
- Discusses specific issues with Active Directory configuration, group policies, multi-factor authentication, and password policies.
- Expresses the need for a comprehensive tool that can assess the effectiveness of security controls from a single pane of glass.

Potential Consequences of Security Gaps:

- Emphasizes the risk of unauthorized access due to ineffective controls.
- Discusses potential consequences, including data breaches, financial risks, reputational damage, and violations of privacy laws.

Existing Solutions and Gaps:

- Expresses difficulty in finding a tool that consolidates data from various security controls to provide a holistic view.
- Highlights the importance of a tool that can address the challenge of maintaining an accurate CMDB (Configuration Management Database).

Collaboration with Cyber Innovation Hub:

- Envisions a collaborative effort to dive deep into specific use cases.
- Emphasizes the need for understanding how different solutions work together and the technicalities involved in integration.
- Proposes a workshop or brainstorming session to gather thoughts and articulate pain points.

Measuring Success of a Solution:

- Defines success as zero audit findings, indicating proactive identification and remediation of control deficiencies.
- Suggests weak passwords as a potential Key Performance Indicator (KPI) and emphasizes the need for both technical and business metrics.

Consideration of Procuring a Solution:

- Expresses a strong interest in procuring a solution that addresses the identified challenges.
- Believes such a solution has the potential to solve a significant pain point for cyber leaders.