**Public Sector Future WWPS Podcast Series**

**Project: Public Sector Future WWPS Podcast Series**

**Detail: Episode 60**

**Talent: Alvaro Vitta [host], Jonathan Cassar [guest]**

**TRT: 20:51**

**OLIVIA NEAL**: Hello and welcome to Public Sector Future. This is a show for anyone who cares about using technology and digital approaches in the public sector to deliver better outcomes.

I’m your regular host, Olivia Neal, and today we’re continuing with the third of our episodes focusing on cybersecurity.

Today, we’re joining Jonathan Cassar who is the Chief Technology Officer of Malta's IT Agency. Along with our cybersecurity guest host Alvaro Vitta, Jonathan shares his experience in integrating modern technology tools, like hyperscale cloud, automation, AI and machine learning, to build a modern government security operations center, which can be effective in defending against those increasing threats we've been hearing about in recent episodes. Jonathan gets very practical in explaining the components of a successful strategy, and the mission and value of a role in defending a nation's cybersecurity.

Let's get into the conversation. Alvaro, over to you…

[TCR 0:00:01]

**ALVARO VITTA:** Jonathan, for our global audience, can you provide a brief description of your role and what you and your team are responsible for in the government of Malta?

**JONATHAN CASSAR:** I’m Jonathan. I am Chief Technology Officer and head of Information Security for the Malta Information Technology Agency. MITA basically is the government IT agency responsible for government digital workloads, infrastructure, network and cybersecurity.

My department, apart from the CTO’s office, the security department is responsible for the cybersecurity of the digital assets of the workloads we host for government in our data center, and of the other workloads, which we host on our hybrid cloud as well.

So and my team is responsible for security governance, compliance, risk assessments, incident response, and security operations center.

It’s good to mention as well that we have a team which is the National Cybersecurity Coordination Center, responsibility for cybersecurity awareness at the national level, and also for running funding programs for small businesses and the service as well.

**ALVARO VITTA:** looks like you have a lot of responsibilities.

So Jonathan, when we look at the cybersecurity global trends, specifically in public sector, what we notice is that nation-state sponsored activity has increased dramatically over the last year, with 53% of all activity targeting government and critical infrastructure organizations. And then on the cybercriminal side of the house, we see public sector also being the number one target of ransomware attacks. So it seems like there’s a lot of cyberthreat attention against public sector organizations. So in your opinion, what makes nation-state actors and cybercriminals see government organizations as a prime target for these attacks?

**JONATHAN CASSAR:** Well, definitely most public sector organizations hold sensitive information. We speak about personal data and things related to national security, intellectual property, related to – to research, financial records. And I’m sure that this data is very much of interest to the different actors at play.

We also provide essential services and infrastructure such as healthcare, education, energy, transportation, sometimes communication. So if a threat actor managed to disrupt the service and infrastructure, obviously there are consequence for the public safety, for the economy, even sometimes for the social stability of a country or region.

Also, when speaking about public sector organizations, we’re talking about very complex organizations . Obviously, this creates an environment which sometimes is challenging in terms of coordination, collaboration, governance, oversight of policies. And this obviously helps these threat actors to see us as a very good target.

**ALVARO VITTA:** Thank you, Jonathan. Yeah, definitely, we see similar things across other governments. There’s a lot of challenges, of course, around the fragmentation of security services, and also the sheer size of the different government entities and the difference in roles that they have. And sometimes it’s just very complex to coordinate and orchestrate the cybersecurity monitoring and response to these entities.

**JONATHAN CASSAR:** Definitely different departments and ministries also have competing priorities. I mean, they are mainly concerned with running their business and reaching their business objectives related to their vertical.

And sometimes cybersecurity doesn’t get the same priority as the other business objectives. We’re getting there, but obviously, it takes time.

**ALVARO VITTA:** No, that makes sense. And basically what you’re saying is that, you know, they’re in the business of running government and running their organizations. They’re not in cybersecurity business. And hence, it doesn’t take a priority. And so that makes a lot of sense.

So, Jonathan, from your perspective, how can government operated security operations center be an opportunity to start helping these government entities and mission critical infrastructure organizations to be able to prepare for and respond to these nation-state threats and cybercriminal activity?

[04:39]

**JONATHAN CASSAR:** First of all, one would need to have some kind of security operations center strategy, which certainly needs to align with the business goals and the risk appetite of the government organizations.

From my perspective, also, as a CTO, I think that we’ve been going through a transformation when it comes to security operations and where the security department is not the function that says no to everything. But it is the function that enables the business to reach its objectives.

So I think the strategy certainly evolves around prioritizing the most secure assets and services, define different roles and responsibility, and also establish an element of metrics and KPIs, where also we can measure the performance of the security operations.

Definitely tooling helps. So one would need very good technology tool stack. Obviously, here the idea is that the more visibility you have, the more detection capabilities you have, and the more responsibility capabilities you have across whole environments, the more risk you are able to take.

So if I have no visibility on a particular system, I don’t know what’s happening. I’m not inclined to take any risks over there. But if I increase my level of visibility, and I know what is happening, and I know that I have certain response capabilities, and I am open for more risk, or I’m open to implement different things, because there as long as I have the visibility, then I have the capabilities to prevent, detect, and respond. So I think that is part of an important aspect when it comes to a SOC strategy.

Obviously the same things when it comes to people, process and technology still apply. So one still needs to have in the IT infrastructure according to standards, follow a number of frameworks, either NIST or ISO. There is the need, obviously, to conduct regular vulnerability assessments and penetration testing, threat hunting and auditing. I mean, these are things which still need to be in place.

Also, last but not least is the element of the human factor and the cybersecurity training and awareness. I think people are one of the first defenses and the last defenses when it comes to cybersecurity. Most attack vectors we see come through emails or social engineering, where the person, the human plays an important role there to manage to stop this particular attack chain. So I think education and awareness are just as important as the processes and the technology partner as well.

[07:33]

**ALVARO VITTA:** And I agree, I think that overarching visibility allows you to have the periphery in order for you to be able to make the right decisions with the resources that you have. And it’s that integration of people, technology, policy and process modernization that allows you to have the agility to be able to effectively manage a government security operation center.

So, Jonathan, when we look at the people aspect, when you touched on that very eloquently, and we see that in the market today, right, there’s 3.5 million unfilled positions on cybersecurity globally through 2025, right, and government organizations have to compete with private sector companies for this talent. And of course, they’re at a disadvantage because of the nature of how public sector and private sector organizations go after this talent and the compensation, and so on and so forth.

So what do you think government organizations can do to attract and retain cyber talent? Are there best practices that you’re seeing across your country and your organization and the peers that you work with in the region?

**JONATHAN CASSAR:**

In reality, as a government organization, we do not really compete with the private sector when it comes to compensation and benefits.

However, there are other things which are important when we’re working for an organization, such as ours. So in our case, we do provide one of the largest wide area networks in the country. We have the largest IT infrastructure. We have the largest data center. So people working here really get a lot of exposure, they get a lot of opportunities for growth, for rotation, and for promotion. We use different platforms and different technologies. So there is a lot of space for learning new things.

Obviously, there’s also the element of what’s our mission, and what’s our impact on the public and the citizens. we’re serving the public good, and we’re protecting national security, we’re enhancing public safety, , we’re also providing a better life for our citizens. So for persons looking for the kind of mission, for the kind of cause, that is how we can attract that kind of talent.

Obviously, where culture is very important as well, and especially when it comes to cybersecurity, fostering teamwork collaboration is very, very important.

As we all know, apart from the large gap in skills and in resources, it’s very important that we also prioritize mental health. We’ve seen lots of problems related to mental health, especially in the cybersecurity sphere, due to different pressures, long hours, the different hours of incident response, so there is a lot of pressure there.

And I think fostering a positive work culture, where you find the support and collaboration that you need to be effective in your work, I think is another important element when it comes to choosing where you work and how also you can attract and retain talent when it comes to cybersecurity.

[11:18]

**ALVARO VITTA:** And I think it’s great in the way that you put it, in that, you know, cybersecurity talent is usually mission oriented. And if you provide an environment where they can grow, they can fulfill that mission, they have purpose, and when they’re doing so in an environment that offers the technology and the cultural elements that allow them to be at the leading edge of that technology spectrum, it gives him a lot of appetite to say, okay, I am growing in this organization, I am providing value, I have purpose, and at the same time, the organization value my skills, and it’s investing in me. And therefore, I want to stay here because I’m growing and participating in the cybersecurity ecosystem, and it’s a win-win situation. So I think that’s a great strategy for others to follow.

Now, as you look at a national level, right, and you have a lot of entities, and you have a lot of different things to manage, right, one of the things that we’ve noticed is, of course, over the last few months, there’s been a significant advance in generative AI capabilities. And cybercriminals have been early adopters of this technology. So they’re already using hyperscale cloud. They’re using automation. They’re using this generative AI to weaponize and monetize these nefarious activities against government organizations, right.

So from your perspective, what can government organizations do in this technology spectrum, to be able to level that playing field, given the advanced sophistication that these cybercriminals and nation-state actors are adopting?

**JONATHAN CASSAR:** So what we mentioned before, the age of technology policy and people who are adopting and implementing cybersecurity best practices, standards, investing in education and workforce development, address skills gap, enhance the collaboration and information sharing still apply.

However, we are firm believers as well of fighting fire with fire. So we really need to also adopt and implement advanced and integrative technologies, which help us provides comprehensive and timely visibility and detection and response capabilities.

I think this is the best use case for the application of AI from all of that and will help to enhance the levels of automation response orchestration across the different platforms, like security information, event management, endpoint detection and response and threat security monitoring. So I believe that having the same kind of tools and capabilities that the threat actors have is very important to be able to defend and respond against these capabilities.

You mentioned the use of hyperscale and artificial intelligence. Most organizations, and especially government organizations with large infrastructure, they generate a lot of data, a lot of security events, and a lot of event data, that it will be humanly impossible to go through and on a manual basis.

So this is why we apply tools using AI and machine learning where we’re establishing baselines. We’ll create what we call patterns of life, and monitor any deviations from those patterns, and those baselines.

So let me just give one example. When it comes to identity monitoring, I use my identity in the morning from my office, and then after an hour, my identity is used from a different country. It would be a case of impossible travel. So that is an anomaly that is flagged, detected, and then investigated, and any deviations from normal baseline is investigated in the same way. This can only be done by using artificial intelligence and the use of hyper-scale and cloud to be able to consume and processes such large amounts of data.

So yes, AI does provide lots of challenges, but it also provides lots of opportunity for us to be able to detect and respond in adequate and capable manner.

[15:50]

**ALVARO VITTA:** Thank you, Jonathan. And I applaud your method of saying, listen, let’s fight fire with fire. If they’re using hyperscale cloud, if they’re using automation, machine learning, if they’re using artificial intelligence, we need to do the same in order to keep up. Otherwise, we would be at a disadvantage. And this allows us to be able to level that playing field, right, and I think is a great message that other government organizations should follow, so that they can then be effective at defending based on the scale, sophistication, the volume of these attacks, right? It’s the only way, as you mentioned, right? You cannot just use humans for this. You need humans. Plus, you need this technology in order to counter these threats.

So, Jonathan, when we look at best practices, when you look at the automation of your security operation center in government, right, what activities do you recommend other to do? What steps do you recommend them to do in order to be able to do what you’re doing, which is, you know, automated incident response, threat hunting, user behavior analysis, using machine learning, using hyperscale cloud? What are some of the things that you recommend other governments to start thinking about as they get into the journey of modernizing their government security operation centers?

[17:21]

**JONATHAN CASSAR:** Yes, I think that one of the first principles is to have a capability to detect threats through all stages of an attack. This can be done by using technologies like endpoint detection and response, network security monitoring, and security information event management. The data needs to be collected, analyzed from the various sources and there be able to identify malicious activities across the whole chain.

It’s important to investigate all others. Again, humanly it’s not possible without these kinds of tools. But it’s important to investigate all others to ensure that nothing is overlooked.

Again, this can be done by using technology such as orchestration, automation, and response, and use artificial intelligence to help you triage, prioritize, and also enrich the alerts with contextual information and threat intelligence.

We need the capability to also gather forensic evidence for investigation remediation. Again, the same technologies come in play.

And most of all is being able to leverage security automation. SOC analysts can get tired when filtering through events, and it’s important to automate repetitive and manual tasks, such as correlation, enrichment and validation.

There are also a number of containment, eradication and recovery responses that can be done and automated as well. So I think whatever can be automated, it is important that we look at those opportunities, so even the SOC analyst can free their time, can free their mind to do activities which add value, to do activities related to the engineering side on how to improve the interactions and improve the automations themselves.

Obviously, we need to make very good use of threat intelligence, using different threat intelligence platform, and be able to consume those threat intelligence sources into actionable items, such as indicators of compromise techniques, and procedures.

Here, it is very important, the element of collaboration. You can’t work on your own, but threat intelligence needs to come from different sources. So it’s important to have a number of agreements with different agencies, with through partners who can provide you with this information, and that you provide them with similar information.

Also, as much as we can, we need to combine the available data that we have across silos. It’s important to use cloud-based platforms, which help us aggregate and normalize the data from different security information security tools, so that we have an overview and an overall visibility of our infrastructure and what is happening.

Obviously, automation does not mean replacing human analyst with AI or machines, but it’s a matter of augmenting our human capabilities to better achieve our outcomes.

[20:18]

**ALVARO VITTA:** That is excellent, and I applaud you and your team for the incredible work and your incredible, innovative mindset around these incredible complex domain which is cybersecurity.

So we want to thank you for your time today, and thank you for sharing your incredible insights, and for your service and that of your team and what you do to keep government digital assets safe. Thank you.

**JONATHAN CASSAR:** Thank you, Alvaro.

Very much appreciate the opportunity to speak to you.

[20:51]

**OLIVIA NEAL:** Thank you to our guest, Jonathan Cassar, and to guest host Alvaro Vitta, and thank you to you for joining me today on Public Sector Future. Visit our website at aka.ms/publicsectorfuture to find more insights and material on cybersecurity, and do go and check out our recent episodes with Tom Burt and Sami Khoury if you haven't yet. As always, please do send us your questions and feedback, you can find me, and Alvaro, on LinkedIn, or email us at [ask-ps@microsoft.com](mailto:ask-ps@microsoft.com). Thank you and see you next time.

END