Interview – Dr Mel Griffiths PhD, Security Operations Manager and Cyber Security Expert

Team Interview 2 July via MS Teams Video Meeting 9pm to 9:55pm

Dr Mel introduced himself and explained a little of his career and education history before we commenced the questions:

Dr G:

- Started off my career in Security Science working for Local Government
- Completed a Bachelor of Counter Terrorism and Security Intelligence
- Then did Honours in Security Science
- Completed a PhD in Security Risk Perception – How we perceive risk and our emotional response to risk. For example, some things of equal risk are considered by an individual differently according to when they occur. People may be willing to buy a home near an electricity substation; however, if a proposed electricity substation is to be built near existing homes there will typically be a huge outcry.
- In 2018 completed a Graduate Diploma in Cyber Security and made the career pivot into Cyber Security.

Team: Why did you make that career pivot (to Cyber Security)?
Dr G:

- It was hard to find tenure in Academia due to long tenure of people already in the positions who had no intention to leave or plans to retire.
- The move to Cyber Security seemed like a more relevant and more accessible role to attain in the 21st century.

Team: What kind of work do you do?

Dr G:

- I am Head of Security Operations Centre (SOC) at Sapien Cybersecurity in Perth.
- Sapien is a small start-up company, with less than 30 people currently employed.
- Sapien Cyber Security installs and manages Threat Management and Vulnerability Management Systems aimed at the Operation Technology (OT) Sector: The OT Sector is anywhere in the real world where Operational Technology meets the real world *e.g. mining trucks, water utilities, power and oil and gas.*
- Sapien Cybersecurity currently look after clients in oil, gas, mining, chemicals. Sapien is looking to work with the Department of Defence; specifically, their OT fuel farms
- I complete a lot of development and research on the companies we work for and the ones we want to work for.

Team: Where do you spend most of your time?

Dr G:

- Spend most of my time in the Security Operations Centre because I manage Security Analysts in the aspect of the business where we actually deploy the Cyber Security products/systems.
- The structure of Sapien is such that there is an Executive Team and underneath that Head of Security Operations (me) and the Head of Development. We both manage the Operations Team and within that I manage the Security Operations Team.
- I would summarise my work time as a 50/50 split between product development and client service.

Team: A fair cohort of our class is interested in Cyber, do you think this industry is flooded or do you think there is ample room and how can we succeed?
Dr G:

- There is ample room as it's a growing industry.
- Finding people with a sufficient skillset is the hardest part.
- We find Recruitment Advertising returns hundreds of applications, but none are near the experience / certification levels expected.
- Once you're able to get your foot in the door, you are usually set and, on your way, to landing a good job in the industry.
- Industry Certifications are valued as is work experience. Recommend you tailor your resume and even volunteer to do unpaid work experience.
- To train I set up multiple virtual machines at home and used the tools to hack one virtual machine from the other so I could see what the impact was and test ways to avoid the hack.

Team: What other tools would be good for training?
Dr G: The best operating system is Kali Linux which is a version of Linux kitted up with a huge suite of penetration testing and hacking tools for ethical hacking.
You should also check out the Mitre Att&ck Framework – this is like a large table of attack vectors and methods and what are the advanced persistent threats
"Getting Started with Att&ck" Adam Pennington, Andy Applebaum, Katie Nickels, Tim Schulz, Blake Strom & John Wunder
https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf need to cite this in text and then do Harvard referencing. Retrieved from mitre.org on 8/7/2020

Team: What kinds of people do you interact with: Other IT professionals? Clients? Investors? The general public?

Dr G:

- I interact with three major areas: Security Operations Centre (SOC) team, Operations team, Development team.
- I report to the Overarching Executive Team so I meet with them.
- I give instructions daily to the SOC team. The SOC team monitors the client's businesses using security products and looks for IOCs (Indicators of Compromise) – our researchers will look at a file and "hash it" (one way encrypt to get a specific encrypted result) to get a fingerprint and then compare it with any file that has an Indicator of Compromise to see of the hashes match. We then pass this information through to clients.

- One of the types of tools we monitor with is an Intrusion Detection System: it sits with the firewall. It monitors traffic going through and takes a mirror image of the system frequently and via machine learning, grows its "understanding" of what that client's normal traffic looks like; therefore, becoming better at finding anomalies or IOCs.
- I connect with the Development team for Research and Development.
- I liaise with clients to report security events, monthly reporting, establishing processes, client training.
- I also liaise with prospective clients by providing product demonstrations.

Team: What aspect of your work do you find most challenging?

Dr G: The product development part of the role is the most challenging. The biggest vulnerability in Security is Layer 8 – people – particularly the people within an organisation creating vulnerabilities for attackers (mostly unintentionally but also intentionally).

Phishing attacks are huge now and people are definitely the weakest link, Ransomware is growing with hostile states (one in particular) employing it to raise capital. I emphasise with our clients and advise all to invest in their staff and in staff security education.

Hackers are always changing and are always going to be more agile. The best hackers use your own network's access and tools against the network itself. Many hackers are in the system just watching and learning for a long time, even years, before they launch an attack.

Team: Are there ever any cultural or language indications left in hacking attempts that may give an indication of the country of origin of the hacker?

Dr G: Well different keyboards would be a possible indication. For example, the Russian keyboard layout will show in the network traffic. However of course this can be faked to make it look like a certain state-based actor was the perpetrator. Sometimes state based hackers will leave a subtle calling card because they want the target to know who hacked them. Security analysts can often tell if it was a particular state by the type of information they are stealing.

Hackers will sometimes leave traces of their tactics. If you can observe and learn a hacker's behaviours, tactics and procedures and deny access to those you are most effective fighting off that hacker because they have to make the hardest change, which is learn new behaviours. You should Google "Pyramid of Pain" (we did see Figure 1) as it gives a good indication of the most effective threats to a hacker (at the top: Tactics, techniques and procedures https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html retrieved 8//7/2020 posted 2 March 2013 by David J Bianco.

But it's important to remember that most hacking attempts are financially motivated (theft or industrial espionage).

Team: **Finally, can you share an example of the work that you do that captures the essence of the IT industry?**

Dr G: The essence of the IT industry is that it is a constantly and rapidly evolving field. The evolution and ubiquity of computing in the information age means that IT is interwoven into every aspect of life. An example of the work that I do that captures the essence of the IT industry is my company's interest in protecting the security interests of Operational Technologies that operate utilities, oil and gas, and many other industries.

Team: Thank you so much Mel.