Name: Luke Morgan

Student number: S3980747

Student email address: s3980747@student.rmit.edu.au

Githubpages https://lukedeninmorgan.github.io/Assessment1/

Github repo:
https://github.com/LukeDeninMorgan/Assessment1.git

About me: I am 28, born and raised in Byron Bay, a hardcore gamer and very interested in cyber security. I have a mug collection and I like cute things. Technically I have played Dota 2 competitively but didn't get very far.

Education: Certificate IV in cyber security Tafe QLD (2022)

High school Certificate (2012)

My interest in IT has been slowly growing since I was younger playing games on my home computer when I was around 12-13. When the pandemic first started affecting Australia, I lost my full-time job. I struggled to find a career path that I wanted to follow, then I stumbled into the job trainer program and jumped at the chance to study cyber security. Ever since starting my Certificate IV in cyber security. I have been very interested and seeking a career in Cyber security. Firsthand experience using various cyber security tools in assessments such as: Creating multiple virtual machines set up on one physical computer so I can simulate a man in the middle attack to grab unencrypted credentials with Wireshark, creating and preforming a red vs blue incident response team exercise. These hands on assessments really drove my hunger to continue to learn more about IT and cyber security. I have no formal IT work experience.

I chose RMIT as I found that the online model of learning suited me better than on campus. I enrolled through online university's Australia and RMIT is the university that they do it through. RMIT is a highly regarded university when it comes to IT, so employers will look at a degree from RMIT favourably.

I expect to learn a range of aspects of IT: More in depth programming skills; better ways at communicating to co-workers/clients; Cyber security; Data science; Networking; Business Analytics and more!

Ideal job

Cyber Security Manager

Share

Morgan Consulting

Mascot, Sydney NSW
Security (Information & Communication Technology)
$200000 - $280000 per annum • Full time

Posted 1d ago

More jobs from this company

Quick apply Save

The Company

Diverse, enterprise organisation which is in a growth phase. Offering an attractive salary plus a bonus component, which was paid during the pandemic. This value-driven company is dynamic, complex and fast paced.
Offering free parking and a hybrid working environment, this organisation promotes collaboration and respect and is less focused on hierarchy.

The Role

Responsible for the day-to-day running of all of the Cyber Security business unit, including governance, risk & compliance (GRC), as well as operations, processes and the more technical aspects such as incident response. Leading a team of 7, with 5 direct reports, you will be a thought leader who will provide subject matter expertise to both internal & external stakeholders.
This organisation is ISO 270001 certified and whilst the security posture is relatively mature compared to other organisations within the same sector, the role is integral to protecting the company from cyber attack.

Skills & Experience

- Extensive experience in a Cyber Security leadership role, within a complex environment
- Leadership experience, both from a management perspective as well as being a thought leader
- Proven experience across GRC, data loss prevention (DLP), modern cyber toolsets, next generation firewalls etc.
- Motivated, self-driven with strong problem solving skills & ability to deal with ambiguity, adapt to change and prioritise
- Focused on continuous improvement and with a passion for learning
- Ability to manage an outsourced SOC
- Tertiary Degree in IT or other relevant discipline
- Industry Certifications relevant to this role will be advantageous

MUST be an Australian Citizen, Permanent Resident or have full working rights to be considered for this position.
There is also a requirement to be fully vaccinated (3 shots including booster) for Covid.

Interested? Please APPLY ONLINE.
Specific questions, ideally after submitting your resume, can be directed to Leonie Jennings on (03) 8606 0305.
REF: V-41719.

Link to job: https://www.seek.com.au/job/58360980?cid=ios-share

Ideal Job cont.

This position is at the top of the cyber security roles in this company. The role involves running the Cyber security business unit, incident response, GRC, leading and managing a response team. This position is appealing to me as I have thought of myself as a leader, is a senior cyber security position, and the pay is impressive.

This role requires: Previous experience in a cyber security management role such as CSOC manager; Experience in Governance, Risk and Compliance (GRC); Data Loss Prevention (DLP), cyber security toolsets and firewall configurations. Ability to manage a Cyber Security Operations Centre (CSOC) Must be Motivated, self-driven, focused on continuous improvement, have strong problem-solving skills and able to adapt to changes. Finally, this role also requires a tertiary degree in IT or related discipline and any industry certifications related to cyber security would be beneficial.

The experience, skills, and qualifications I currently have are as follows:

I have a certificate IV in cyber security (Tafe QLD 2022) as well as: leadership; mentoring; and managing experience; strong customer and client service skills; I am always looking to improve myself and gain new skills or knowledge especially when it comes to cyber security. My experience, skills, and qualifications and on the path towards what is required for the Cyber Security manager position but are not there yet. I still require experience in a Cyber Security leadership role, more experience in governance, risk and compliance and data loss prevention. I also require more training and knowledge in cyber security toolsets, processes, and firewalls. I do however already have an industry Certification related to cyber security.

The path I should follow to be a candidate for this position is:

Complete and attain the bachelor's degree in information technology from RMIT.

Complete and attain the master's degree in cyber security.

Once I have my Bachelor's/master's degree, I can search for a job in a cyber security operation centre (CSOC) as an analyst and gain some hands-on experience. While working as a CSOC analyst or similar I will work towards industry certifications such as the CISSP certification.

After working as a CSOC analyst or similar for a few years, I will find a new role higher up as a manager of a CSOC or similar. After working as a manager of a CSOC or similar I should have the required experience and skills to be a candidate for the Cyber security Manager position.

Personality Profile

Result of an online Myers-Briggs test: ISFJ-T (Defender)

Result of an online learning style test: Visual learner 50%/ tactile learner 30%/ Auditory 20%

Result of big 5 online personality test: Openness to experience – Medium characteristic

Extraversion – Low Characteristic

Conscientiousness – Medium Characteristic

Agreeableness –High Characteristic

Neuroticism – Medium Characteristic

Your Results

Defender

ISFJ-T

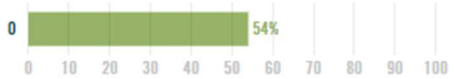
Sentinel

Constant Improvement

35%	EXTRAVERTED	65% INTROVERTED
48%	INTUITIVE	52% OBSERVANT
29%	THINKING	71% FEELING
63%	JUDGING	37% PROSPECTING
39%	ASSERTIVE	61% TURBULENT

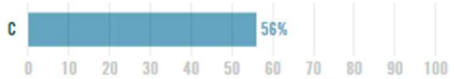
Openness

Openness describes a person's tendency to think in abstract, complex ways. High scorers tend to be creative, adventurous, and intellectual. They enjoy playing with ideas and discovering novel experiences. Low scorers tend to be practical, conventional, and focused on the concrete. They tend to avoid the unknown and follow traditional ways.



Conscientiousness

Conscientiousness describes a person's ability to exercise self-discipline and control in order to pursue their goals. High scorers are organized and determined, and are able to forego immediate gratification for the sake of long-term achievement. Low scorers are impulsive and easily sidetracked.

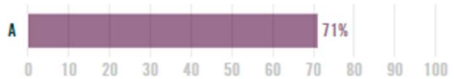


Extraversion

Extraversion describes a person's inclination to seek stimulation from the outside world, especially in the form of attention from other people. Extraverts engage actively with others to earn friendship, admiration, power, status, excitement, and romance. Introverts, on the other hand, conserve their energy, and do not work as hard to earn these social rewards.

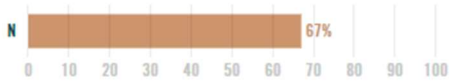
Agreeableness

Agreeableness describes a person's tendency to put others' needs ahead of their own, and to cooperate rather than compete with others. People who are high in Agreeableness experience a great deal of empathy and tend to get pleasure out of serving and taking care of others. They are usually trusting and forgiving. People who are low in Agreeableness tend to experience less empathy and put their own concerns ahead of others.



Neuroticism

Neuroticism describes a person's tendency to experience negative emotions, including fear, sadness, anxiety, guilt, and shame. While everyone experiences these emotions from time to time, some people are more prone to them than others. High Neuroticism scorers are more likely to react to a situation with fear, anger, sadness, and the like. Low Neuroticism scorers are more likely to brush off their misfortune and move on.



What's Your Learning Style? The Results

Your Scores: Printer Friendly Version

- Auditory: 20%
- Visual: 50%
- Tactile: 30%

You are a **Visual** learner! Check out the information below, or view all of the learning styles.

Visual

If you are a visual learner, you learn by reading or seeing pictures. You understand and remember things by sight. You can picture what you are learning in your head, and you learn best by using methods that are primarily visual. You like to see what you are learning.

As a visual learner, you are usually neat and clean. You often close your eyes to visualize or remember something, and you will find something to watch if you become bored. You may have difficulty with spoken directions and may be easily distracted by sounds. You are attracted to color and to spoken language (like stories) that is rich in imagery.

Here are some things that visual learners like you can do to learn better:

- Sit near the front of the classroom. (It won't mean you're the teacher's pet!)
- Have your eyesight checked on a regular basis.
- Use flashcards to learn new words.
- Try to visualize things that you hear or things that are read to you.
- Write down key words, ideas, or instructions.
- Draw pictures to help explain new concepts and then explain the pictures.
- Color code things.
- Avoid distractions during study times.

Remember that you need to **see** things, not just hear things, to learn well.

https://my-personality-test.com/personality-type-indicator

http://www.educationplanner.org/students/self-assessments/learning-styles-quiz.shtml

https://www.16personalities.com/isfj-personality

The above online test results seem to be very accurate.

I believe myself to be an ISFJ-T(Defender) and Visual learner, Somewhat open to new experiences, very conscientious, a little extravert but mostly introvert, very agreeable and have a tendency to feel negative emotions . As an ISFJ-T I am Hardworking and devoted, with a strong sense of responsibility. I Provide care and support of my friends and family, with a strong eye for detail. I have always through I was a visual learner, but I also learn well with hands on experience. I Generally like to stay with in my comfort zone, though I do like to try new things sometimes, as an extravert, I can gain energy from being social, but also from being alone. It really depends on what the social event is and on the other hand going for a walk alone with some music is great. I feel that I have good control over my emotions in most situations.

The results of these tests show that in a team I can be counted to meet deadlines, will work well in a team due to my well-developed people skills, and that I probably will not seek recognition of the effort I put in. I should be able to keep cool and work well under pressure and time restraints, attending meetings will most likely cause some level of anxiety and use a lot of energy.

When forming a team, I should look for others like me; people that are aware of the deadlines. People in the team should understand each other's boundaries and limits to not over stimulate or reduce each other's energy. Having a more collaboratory group where we all work together instead of competing. Though there should be one designated leader as all groups should. This will provide me with the best possible group environment so we can all produce the best project we can.

Project Idea

Overview

My project idea is a company that performs companywide penetration testing but specialling in Physical/Environmental and internal threats. There is: physical/Environmental; web; network; internal; external; social engineering; white; grey; and black box penetration testing.

What makes my idea different is that not only is it a combination of: physical/Environmental; internal; social engineering and internal network security. We proceed under the black box penetration testing guise. Once a client has paid for our services, we us an "accomplice" that will be aiding our testing from the inside. Just like if there was a real internal threat. Not only that. Depending on the scope of our service (we recommend a 1-year service). We will plan with our contact, but no one else in the business will know a thing to generate the most authentic response. Our focus is the physical/Environmental and the internal threats, as these are often overlooked. With a yearlong approach, all previous breach attempts and knowledge gained from them are combined into 1 final attack where we use all that we have learnt about the business to conduct a companywide breach.

Motivation

I am motivated to create this project as I am very interested in cyber security and penetration testing. Creating the documentation and processes will be interesting. If the project is successful, it may become my business or a business model I will adapt in a business I may create in the future. With the rise in cyber criminals using ransom ware and phishing attacks during the pandemic companies have improved network security and education to reduce the effectiveness of those types of attacks. Physical/Environmental, internal, and social engineering security is often overlooked, having a business's focus around those weaker points will fill a gap in the market and overall strengthen the visibility of those exploits and vulnerabilities.
https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/

Description

The project is a business model that performs companywide penetration testing but specialling in Physical/Environmental and internal threats. So that means, that a client will receive web; network; internal; external; white; grey; and black box penetration testing but will have their physical/environmental and internal security scrutinised. The way we test internal threat protection is by using an "accomplice". The "accomplice" is a current employee that receives a paid incentive to preform actions on our behalf. We first start will a small task, such as find a window that can open, and will increase the threat of the action (We will never ask the accomplice to damage or remove anything that will harm the business in any way and will only use photo evidence when presenting findings). The accomplice may also aid us in leaving security doors open for our technicians to gain access, this is where the need for the combination of physical and internal security becomes apparent.

If our operation scope is as we recommend (1 year service, and all areas of penetration testing). We normally start off our recommended service with a thorough reconnaissance of all outer lays of the company. This includes: the companies' websites, physical and wireless networks access points, physical security of the companies building and looking for points of compromise. A point of compromise is the point where public meets private (normally a door, window, or fence). These vulnerabilities will be rated: Protected (protected from a breach or weather), safe (unlikely a breach

could occur), unsafe (security is in place, but is lacking and a breach could occur) or unprotected (no security, a breach could happen anytime). Following the reconnaissance phase, we will plan at least 1 attack a month minimum, where we attempt to gain access to any valuable resources, gain entry to restricted areas, gain access to the internal network, use our accomplice to aid us in the breach though most likely we will use a combination of them to have the most effect. After each attempt, we list areas that were vulnerable or areas we were able to breach or where the accomplice had access. If these vulnerabilities are within the acceptable levels indicated in the scope, they will only be recorded and used later by our team. If the vulnerabilities are outside of acceptable levels, they will be immediately reported to the company and not used for farther testing. This all leads to the final attack, where we use all the information, we have gained from all the following breaches to attempt a company wide breach. This company wide breach will affect all aspects of the company and involves all areas of penetration testing. We will attack every vulnerability we have found all at once we do this when the company will not suffer as much from any down time from websites opr services. Once we have conducted our final breach attempt. We will document everything and prepare for our meeting with the company where we will explain our findings, our accomplishments, where security is strong or needs improving. We may also be used for educating employees around social engineering and what to look out for with phishing emails.

Tools and Technologies

Our company uses social engineering through social media and other publicly accessible websites. Depending on how the complexity of the client company's security, we may use the following to attempt a breach: public physical access, using stolen credentials at check points or to gain access to secure locations or resources, using social engineering to try pass as employees or third parties to gain access. We may also use RFID badge/ID card signal duplicators to trick sensors to gain access. We will need to have our go bags ready with a laptop running windows/Kali Linux tooled up to collect any unencrypted credentials or to access the network physically or via wireless; port sniffing; vulnerability scanning; website spidering etc.

Skills required

Business skills and knowledge, client management and communication skills, network knowledge and skills, Strong social engineering skills. Our technicians will also need to have some physical capability as they may need to climb fences or squeeze in tight spaces. Ability to perform reconnaissance and operate the tools needed for reconnaissance. All penetration testing skills (physical, environmental, web, network, internal, external, social engineering). Skills related to RFID card readers and duplicators, signal jammers, signal grabbers and replicators. Skills in public speaking, for presenting findings to clients. lecturing, coaching, and teaching skills for educating client companies employees.

Outcome

The expected outcome from this project is to see if this business model would be viable, if it would be able to penetrate the market and be lucrative. If this project is a success, I may continue to develop it and create a business or a business model and adapt it to another business. It will also be

interesting to see how to develop a business such as this and to go through the process of how it is created. If this project is successful, the business created should fill a gap in the market and help businesses better protect their assets and reduce the effect of cyber attacks of business that we service. A business such as this will also highlight the need to better physical/Environmental, internal, and social engineering security.