Unfortunately I am unable to secure interview. Below are the 5 interview questions that I formulated and my reasoning behind them.

Question: To break the ice my first question is what made you interested in cyber security?

Reasoning: The internet touches almost all aspects of daily life. Cyber security has impacts, which extend beyond the digital world and into the physical one. As a cyber-security professional, you'll be working daily to keep critical infrastructure secure, and will constantly be facing new, engaging challenges, from robots to cars to websites serving millions and millions of users, the variety is near infinite. Add together the growth of technology and its variety, and you start to glimpse the different types of puzzles that cyber security professionals can deal with.

Question: What are the most time consuming, challenging and rewarding parts of your job?

Reasoning:

More complex cyber security challenges

Digitalization increasingly impacts all aspects of our lives and industries. We are seeing the rapid adoption of machine learning and artificial intelligence tools, as well as an increasing dependency on software, hardware and cloud infrastructure. Keeping up to date with technology is a bigger challenge.

Fragmented and complex regulations –

Comply with increasingly complex system of regulations and rules, such as the General Data Protection Regulation, the California Consumer Privacy Act and many others worldwide regulations.

Dependence on other parties-

The concentration of a few technology providers globally provides many entry points for cyber criminals throughout the digital supply chain.

Protection for your business –

Cyber security solutions provide digital protection to your business that will ensure your employees aren't at risk from potential threats such as Adware and Ransom ware

Question: How do you see having the right data governance strategy will help minimize cyber security related risk?

Reasoning:

Data governance is the capability within an organization to help provide for and protect high-quality data throughout the lifecycle of that data. This includes data integrity, security, availability and consistency.

To protect against threats, organizations need to know what data to protect and how to help keep it protected. Information protection is at the core of security, but how can you protect it if you do not know what data you have, where your data is, how it is used, whom it is shared with and how it is shared? So, managing your data in a structured, responsible and law-abiding way will make it more efficient for security professionals to protect it.

No organization will be 100% secure, and very few organizations have unlimited resources–people and financial–to implement, operate and improve cyber security measures. Therefore, businesses must take a risk-based approach and focus on the most sensitive data assets.

Question: What does effective cyber security look like to you? How do you measure it?

Reasoning:

There have to be specific ways to measure security efforts in order to determine their effectiveness. Cyber security effectiveness can generally be divided into three areas, these include systems, incidents, and people. Key performance indicators (KPIs) are an effective way to measure the success of

any program and aid in decision-making. Below are examples of
clear KPIs and metrics:

- Intrusion attack - How many times have bad actors attempted to gain unauthorized access?
- Security Incidents: How many times has an attacker breached your information assets or networks?
- Mean Time to Detect (MTTD): How long do security threats go unnoticed?
- Mean Time to Resolve (MTTR): What is the mean response time for your team to respond to a cyber-attack once they are aware of it.
- Mean Time to Contain (MTTC: How long does it take to close identified attack vectors across all endpoints?

There is no hard and fast rule for choosing cyber security KPIs and KRIs. These metrics will depend on your industry, organization's needs, regulations, guidelines, best practices and ultimately, company's appetite for risk.

Question: How can you detect an attempted or successful cyber security incident, brute force attack, or data breach?
Reasoning:
There are many types of cyber security incidents that could result in intrusions on an organization's network such as:

- Unauthorized attempts to access systems or data
- Privilege escalation attack
- Insider threat
- Phishing attack
- Malware attack
- Denial-of-service (DoS) attack

The expanding threat landscape puts organizations at more risk of being attacked. Putting a well-defined incident response plan in place will enable organizations to effectively identify these incidents, minimize the damage and reduce the cost of a cyber-attack.