**[Junior Cyber Security Analyst](https://www.seek.com.au/job/77538891?ref=search-standalone&type=standout&origin=jobTitle" \l "sol=a272108c9a6ce3d0ffec8831bc30e561d9b48291" \t "_blank)**

**Overview**

* **About the Role:**  
  Our client is seeking a motivated and detail-oriented Junior/Entry Level Cyber Security Analyst to support ongoing project work. This is an excellent opportunity for recent graduates or individuals at the beginning of their cyber security career to gain valuable real-world experience   
     
  **Key Responsibilities:**
* Assess and analyse cyber and information security risks
* Implement and monitor security frameworks and policies
* Conduct assurance activities, including gap analysis and threat and risk assessments
* Apply knowledge of industry standards and best practices (Australian Signals Directorate Essential 8, ISO 27001, NIST Cyber Security Framework)
* Utilise experience with SIEM systems, particularly Splunk
* Understand contemporary enterprise IT environments
* Possess knowledge of common cloud platforms and concepts (Microsoft Azure, Office 365)
* **Qualifications:**
* Relevant degree or certification in Cyber Security, Information Technology, or a related field
* Familiarity with SIEM systems, particularly Splunk
* Understanding of industry standards and best practices (ASD Essential 8, ISO 27001, NIST Cyber Security Framework)
* Basic knowledge of enterprise IT environments and cloud platforms (Microsoft Azure, Office 365)

# Interview Script

**Interview Question 1: Assessing and Analyzing Cyber and Information Security Risks**

**Interviewer:** "Can you describe a time when you assessed and analyzed cyber security risks in a project? What approach did you take?"

**Less Effective Response**

**Interviewee:** "I think there was a project where we looked at some security risks. I can't remember all the details, but we checked for some vulnerabilities and reported them."

**More Effective Response**

**Interviewee:** "During my final year project in university, we conducted a cyber security risk assessment for a mock e-commerce platform. I began by identifying potential threats and vulnerabilities, using tools like vulnerability scanners. We then assessed the impact and likelihood of these risks using a risk matrix. By categorizing the risks, we were able to prioritize which ones needed immediate attention. I documented the findings and proposed mitigation strategies, such as enhancing authentication protocols and patching software vulnerabilities. This hands-on experience was invaluable in understanding how to systematically assess and address security risks."

**Interview Question 2: Implementing and Monitoring Security Frameworks and Policies**

**Interviewer:** "How have you applied your knowledge of security frameworks and policies in a practical setting?"

**Less Effective Response**

**Interviewee:** "I studied some security frameworks in class, like ISO 27001. We talked about policies and stuff, but I haven't really done much with them in a real job."

**More Effective Response**

**Interviewee:** "In a recent internship, I had the opportunity to work with a team implementing security frameworks based on ISO 27001 standards. My role involved assisting in the creation and monitoring of security policies. For instance, we developed policies for access control and data encryption. I also participated in internal audits to ensure compliance with these policies, identifying areas for improvement. Additionally, I used my understanding of the ASD Essential 8 to help prioritize controls, particularly focusing on patching applications and restricting administrative privileges. This practical experience has equipped me with a solid foundation in applying security frameworks and policies."

**Interview Question 3: Conducting Assurance Activities**

**Interviewer:** "Can you give an example of a time when you conducted assurance activities, such as gap analysis or threat assessments?"

**Less Effective Response**

**Interviewee:** "In one of my classes, we talked about gap analysis and threat assessments. I remember doing some case studies, but I haven't done much practical work in this area."

**More Effective Response**

**Interviewee:** "During a cybersecurity workshop, I was part of a team tasked with conducting a gap analysis for a hypothetical organization's security posture. We began by benchmarking the organization's current controls against the ASD Essential 8 framework. This helped us identify gaps in areas such as multi-factor authentication and application whitelisting. Following the gap analysis, we conducted a threat assessment to understand potential attack vectors. We used this information to recommend specific measures, such as deploying a more robust SIEM system like Splunk for better monitoring and response capabilities. This exercise provided me with practical insights into conducting assurance activities."

**Interview Question 4: Experience with SIEM Systems, Particularly Splunk**

**Interviewer:** "How familiar are you with SIEM systems, and can you share your experience with Splunk?"

**Less Effective Response**

**Interviewee:** "I've read about SIEM systems and I know Splunk is popular. I haven't used it much myself, but I've seen some demos."

**More Effective Response**

**Interviewee:** "I had hands-on experience with Splunk during a cybersecurity course where we used it to analyze security logs. We set up dashboards to monitor network traffic and identify potential security incidents. One particular task involved creating alerts for unusual login activities, which helped me understand how to configure and fine-tune Splunk's alerting features. Additionally, I completed a Splunk Fundamentals course online, which provided me with a deeper understanding of its capabilities, including its search processing language (SPL) and data indexing features. This experience has given me a solid foundation in using Splunk for security monitoring and analysis."

**Interview Question 5: Understanding of Cloud Platforms and Contemporary IT Environments**

**Interviewer:** "Can you describe your understanding of contemporary enterprise IT environments and your familiarity with cloud platforms like Microsoft Azure or Office 365?"

**Less Effective Response**

**Interviewee:** "I know that cloud platforms are important. I've used Office 365 for schoolwork, but I haven't done much with Azure or other cloud environments."

**More Effective Response**

**Interviewee:** "In my studies and through self-learning, I've gained a good understanding of contemporary enterprise IT environments, particularly the shift towards cloud computing. I'm familiar with Microsoft Azure and Office 365, having used them in various projects. For example, I worked on a project where we deployed a web application on Azure, utilizing its virtual machines and Azure Active Directory for user authentication. I've also explored Office 365's security features, such as data loss prevention (DLP) and advanced threat protection. This exposure has helped me appreciate the complexities and benefits of cloud platforms in modern IT environments."

**Interview Question 6: Handling Security Incidents**

**Interviewer:** "Can you tell us about a time when you had to respond to a security incident? How did you handle it?"

**Less Effective Response**

**Interviewee:** "I haven't had much experience with real security incidents. In school, we talked about what to do, but I haven't done it in a job yet."

**More Effective Response**

**Interviewee:** "During a cybersecurity simulation exercise in my course, I was part of a team that responded to a simulated phishing attack. Our first step was to contain the incident by isolating the affected systems. We then conducted a thorough investigation using SIEM logs to trace the source and scope of the breach. I was responsible for coordinating communication with the 'affected' employees, advising them on steps to secure their accounts and reset passwords. Although this was a controlled environment, it provided valuable insights into incident response procedures and the importance of quick, coordinated action."

**Interview Question 7: Knowledge of Industry Standards**

**Interviewer:** "How do you keep yourself updated on industry standards and best practices in cybersecurity?"

**Less Effective Response**

**Interviewee:** "I sometimes read articles online about cybersecurity. I also follow a few blogs when I have time."

**More Effective Response**

**Interviewee:** "I actively keep myself updated on industry standards and best practices by regularly reading publications from reputable sources like the Australian Signals Directorate and NIST. I subscribe to cybersecurity newsletters and follow industry leaders on platforms like LinkedIn. Additionally, I participate in webinars and online courses to stay informed about the latest developments. For example, I recently completed a course on the NIST Cybersecurity Framework, which deepened my understanding of its practical application in securing IT environments. This continuous learning helps me stay abreast of evolving threats and best practices."

**Interview Question 8: Understanding of Security Tools and Technologies**

**Interviewer:** "What security tools and technologies are you most familiar with, and how have you used them?"

**Less Effective Response**

**Interviewee:** "I've heard of some security tools like antivirus software and firewalls. I haven't used many specific tools in detail, though."

**More Effective Response**

**Interviewee:** "I have hands-on experience with several security tools and technologies. For instance, I've used Wireshark for network traffic analysis and Splunk for log management and security monitoring. During my internship, I worked with the team to set up and configure an IDS (Intrusion Detection System) using Snort, which helped in identifying and responding to suspicious activities. I also have a basic understanding of endpoint protection tools and cloud security features, such as those in Microsoft Azure Security Center. This experience has provided me with a practical understanding of how various tools contribute to a comprehensive security posture."

**Interview Question 9: Team Collaboration**

**Interviewer:** "Can you provide an example of how you worked in a team to solve a cybersecurity problem?"

**Less Effective Response**

**Interviewee:** "In group projects at school, we would work together on assignments. We each did our part, but I usually worked independently."

**More Effective Response**

**Interviewee:** "During a group project in my cybersecurity class, we were tasked with developing a security plan for a hypothetical company. We divided the responsibilities, and I was in charge of assessing the network infrastructure. I collaborated closely with my teammates who were responsible for endpoint security and user training. We held regular meetings to discuss our findings and align our strategies. I also took the initiative to integrate our individual sections into a cohesive security plan, which we presented as a unified team. This experience underscored the importance of clear communication and collaboration in cybersecurity efforts."

**Interview Question 10: Interest and Passion for Cybersecurity**

**Interviewer:** "What motivates you to pursue a career in cybersecurity, and how do you stay passionate about the field?"

**Less Effective Response**

**Interviewee:** "I've always thought cybersecurity is important. I like working with computers and want a stable job in the field."

**More Effective Response**

**Interviewee:** "My passion for cybersecurity stems from a deep interest in technology and a desire to protect sensitive information. The ever-evolving nature of cyber threats and the challenge of staying ahead of these threats excite me. To stay passionate and motivated, I regularly engage in activities like participating in Capture The Flag (CTF) competitions, which provide hands-on experience with real-world scenarios. I also enjoy reading case studies about recent cyber incidents to understand how different industries are tackling security challenges. This continuous engagement helps me remain enthusiastic and committed to contributing to a safer digital world."