**[ICT Cyber Security Analyst](https://www.seek.com.au/job/77498826?ref=search-standalone&type=standout&origin=jobTitle" \l "sol=1f39b9389ee16b4c7d88d72c3eaf91d774797697" \t "_blank)**

ACME has a Non-Ongoing vacancy for an ICT Cyber Security Analyst in the ICT Cyber Security and Assurance Team. This is a fulltime Non-Ongoing role initially for 12 months with the potential to become Ongoing.

A merit pool will be created and may be used to fill similar Ongoing and Non-Ongoing vacancies.

**Overview of Team and Role**

The Technology and Information Management Team facilitates the development and implementation of organisational Information & Communication Technologies (ICT) equipment, services, and related policies to support the delivery of business outcomes.

The ICT Cyber Security Analyst will work to support the delivery of ICT outcomes, specifically within the fields of Cyber Security. The officer will assist with the business as usual (BAU) tasks, development and operation of related policy and procedure, providing assurance to Comcare that its information assets are appropriately protected.

The role will assist with the delivery of effective and highly competent support for the establishment, management, review and administration of ACME’s ICT Cyber Security policies and procedures and ensures both preventive and recovery strategies are in place.

**Desirable Qualifications/Experience**

* A sound understanding and knowledge of IT infrastructure, Networking, Systems, and operating systems will be beneficial.
* A basic understanding of SIEM and SOC solutions will be advantageous.

**Security Clearance**

Ability to obtain and maintain a Baseline Security Clearance.

# Interview Script

**Interview Question 1: Understanding IT Infrastructure, Networking, and Systems**

**Interviewer:** "Can you discuss your understanding and experience with IT infrastructure, networking, and systems?"

**Less Effective Response**

**Interviewee:** "I know a bit about IT infrastructure and networking from my studies. I've worked with operating systems like Windows and Linux before."

**More Effective Response**

**Interviewee:** "I have a solid foundation in IT infrastructure, networking, and systems, gained through both academic coursework and practical experience. For instance, I have worked on setting up and maintaining network infrastructure, including configuring routers, switches, and firewalls. I am also proficient in managing operating systems such as Windows and Linux, where I have handled tasks ranging from user management to system updates and patching. My understanding extends to virtualization technologies and cloud environments, which are increasingly important in modern IT infrastructures. This comprehensive knowledge base equips me to effectively support and enhance Comcare’s ICT environment."

**Interview Question 2: Experience with SIEM and SOC Solutions**

**Interviewer:** "What is your experience with SIEM and SOC solutions, and how do you see them playing a role in an organization's cybersecurity strategy?"

**Less Effective Response**

**Interviewee:** "I've heard of SIEM and SOC but haven't had much hands-on experience with them. I know they are important for security."

**More Effective Response**

**Interviewee:** "During my previous internship, I gained practical experience with SIEM solutions, particularly Splunk. I assisted in setting up dashboards for monitoring and analyzing security events, which provided valuable insights into potential security threats. My understanding of SOC operations includes the roles and responsibilities of monitoring, detecting, and responding to security incidents. I see SIEM and SOC as critical components of an organization's cybersecurity strategy, as they provide real-time visibility into security events and enable a proactive approach to threat management. By correlating data from various sources, these tools help in identifying anomalies and potential security breaches, thus ensuring the protection of an organization’s information assets."

**Interview Question 3: Developing and Operating Cyber Security Policies and Procedures**

**Interviewer:** "Can you provide an example of how you've contributed to the development or operation of cybersecurity policies and procedures?"

**Less Effective Response**

**Interviewee:** "I've read through cybersecurity policies before. I haven't had much experience in creating them, but I know they are important."

**More Effective Response**

**Interviewee:** "In my last role, I was actively involved in the development and operation of cybersecurity policies and procedures. I worked closely with the IT security team to draft a comprehensive cybersecurity policy that covered areas such as data protection, access control, and incident response. I also helped in developing standard operating procedures (SOPs) for common security tasks, such as patch management and vulnerability assessment. These documents were essential in standardizing our security practices and ensuring compliance with industry standards. My role also involved regular reviews and updates to these policies to reflect evolving threats and technological advancements."

**Interview Question 4: Providing Assurance and Implementing Preventive and Recovery Strategies**

**Interviewer:** "How have you contributed to providing assurance that information assets are protected, and what preventive and recovery strategies have you implemented?"

**Less Effective Response**

**Interviewee:** "I've been part of teams that focused on protecting information assets. We used antivirus software and firewalls as preventive measures."

**More Effective Response**

**Interviewee:** "I have contributed to ensuring that information assets are protected by participating in regular security assessments and audits. For example, I conducted vulnerability scans and risk assessments to identify potential weaknesses in our systems. Based on these findings, I implemented preventive measures such as enhancing firewall rules, applying critical security patches, and improving our data encryption protocols. Additionally, I developed and tested incident response plans to ensure we could quickly recover from any security breaches. This included defining clear roles and responsibilities for the incident response team and conducting regular drills to test our readiness. These strategies provided comprehensive protection and assurance for our information assets."

**Interview Question 5: Obtaining and Maintaining Security Clearance**

**Interviewer:** "This role requires the ability to obtain and maintain a Baseline Security Clearance. Can you discuss any experience you have with handling sensitive information and how you ensure compliance with security protocols?"

**Less Effective Response**

**Interviewee:** "I understand the importance of handling sensitive information carefully. I follow the rules and guidelines provided by my organization."

**More Effective Response**

**Interviewee:** "In my previous position, I handled sensitive information regularly, adhering to strict security protocols to ensure data confidentiality and integrity. I was trained in data handling procedures, including the classification of information and secure disposal of sensitive documents. I also followed protocols for secure communication, such as using encrypted email and secure file transfer methods. To ensure compliance, I regularly reviewed and updated my understanding of relevant policies and participated in security awareness training. I am prepared to undergo the necessary background checks and training to obtain and maintain a Baseline Security Clearance, understanding the importance of safeguarding sensitive information in a government context."

**Interview Question 6: Handling Business as Usual (BAU) Tasks in Cyber Security**

**Interviewer:** "Can you describe how you manage and prioritize Business as Usual (BAU) tasks in a cybersecurity role?"

**Less Effective Response**

**Interviewee:** "For BAU tasks, I just follow my daily checklist and make sure everything is running smoothly. If something urgent comes up, I handle it as it comes."

**More Effective Response**

**Interviewee:** "In managing BAU tasks, I prioritize based on the potential impact on business operations and security. I typically start my day by reviewing system logs and alerts to identify any immediate issues that need attention. Regular tasks, such as updating antivirus software and conducting routine vulnerability scans, are scheduled to ensure consistent protection. I also maintain a ticketing system to track and prioritize tasks, ensuring that critical issues are addressed promptly. By balancing routine maintenance with proactive threat hunting, I ensure that our systems remain secure and that any emerging threats are swiftly mitigated."

**Interview Question 7: Working in a Collaborative Environment**

**Interviewer:** "How do you approach working with different teams, such as IT and non-IT staff, to implement cybersecurity measures?"

**Less Effective Response**

**Interviewee:** "I usually communicate with the IT team when there's something important. With non-IT staff, I keep things simple and just tell them what they need to know."

**More Effective Response**

**Interviewee:** "Collaboration is key in cybersecurity, as it often involves cross-functional teams. When working with IT staff, I use technical language to ensure clarity and precision in implementing security measures. For example, while deploying a new firewall policy, I collaborated closely with network administrators to fine-tune the settings. With non-IT staff, I focus on clear and accessible communication, avoiding jargon. For instance, I conducted training sessions on phishing awareness for various departments, using real-world examples to illustrate potential threats. By tailoring my communication style to the audience, I ensure that everyone understands the importance of cybersecurity and their role in maintaining it."

**Interview Question 8: Understanding Cybersecurity Threats and Risks**

**Interviewer:** "Can you provide an example of a cybersecurity threat you encountered and how you addressed it?"

**Less Effective Response**

**Interviewee:** "We've had a few threats come up, like phishing emails. I usually just tell people to be careful and not to click on suspicious links."

**More Effective Response**

**Interviewee:** "One significant threat we encountered was a phishing campaign targeting our employees. The attackers were attempting to steal login credentials through a fake company portal. Upon identifying the threat, I worked with the IT team to implement immediate measures, including updating our email filters to block similar phishing emails. I also coordinated with our security team to conduct a company-wide phishing awareness training, emphasizing how to identify and report suspicious emails. Additionally, we enforced multi-factor authentication for all users, which significantly reduced the risk of credential theft. This proactive response not only mitigated the immediate threat but also strengthened our overall security posture."

**Interview Question 9: Knowledge of Cybersecurity Regulations and Compliance**

**Interviewer:** "How do you ensure compliance with cybersecurity regulations and standards in your work?"

**Less Effective Response**

**Interviewee:** "I know that compliance is important, and I try to follow the guidelines and policies that are in place."

**More Effective Response**

**Interviewee:** "Ensuring compliance with cybersecurity regulations and standards is a critical aspect of my work. I keep myself updated on relevant regulations, such as the Australian Privacy Principles and the Information Security Manual. I conduct regular audits and assessments to ensure that our policies and procedures align with these standards. For example, during a recent audit, I identified gaps in our data retention policy and worked to update it to comply with the latest guidelines. Additionally, I collaborate with the legal and compliance teams to ensure that our security measures are not only effective but also legally compliant. This proactive approach helps protect our organization from legal risks and ensures that we maintain a high standard of security."

**Interview Question 10: Handling Security Incidents and Reporting**

**Interviewer:** "Can you describe your role in handling security incidents and how you report them?"

**Less Effective Response**

**Interviewee:** "When there's a security incident, I just fix the problem and move on. I make sure to tell my supervisor what happened."

**More Effective Response**

**Interviewee:** "In the event of a security incident, my first step is to contain the threat to prevent further damage. For example, if there's a malware outbreak, I would isolate the affected systems and start an investigation. I follow a structured incident response plan that includes identifying the root cause, eradicating the threat, and restoring affected systems to normal operations. Reporting is a crucial part of this process. I document the incident details, including the nature of the threat, actions taken, and any recommendations for future prevention. This report is then shared with senior management and relevant stakeholders, ensuring transparency and facilitating a post-incident review. This approach helps in refining our security measures and improving our readiness for future incidents."