Cyber Security Analyst interview questions

careertips.com.au: common questions and what they're really testing

What to expect

Interviews for Cyber Security Analyst roles usually mix technical depth with judgement calls, since employers need to know you can both run the tools and make sound decisions when something goes wrong. Expect questions that test how you think through a problem, not just whether you know the terminology.

- **Technical:** Questions on how you use specific tools and processes, such as SIEM log analysis, vulnerability scanning or packet capture, to confirm you can actually do the work.
- **Scenario:** A hypothetical incident or judgement call presented on the spot, testing how you prioritise and respond under time pressure.
- **Behavioural:** Past-experience questions about handling conflict, pushback or ambiguity, usually answered with a specific example.
- **Compliance and knowledge currency:** Questions on how you keep up with new threats and regulatory obligations, since the threat environment and Australian compliance requirements shift constantly.
- **Stakeholder communication:** Questions testing your ability to explain technical risk to non-technical staff or management.

Most processes start with a phone or video screen focused on background and motivation, followed by a technical interview with a security lead or hiring manager covering tools and incident scenarios, and often a final round with a senior manager or business stakeholder to assess communication and fit. Some employers include a practical exercise, such as analysing a sample log file or writing up a mock incident report.

1. Walk me through how you would investigate a spike in outbound traffic from an internal server flagged by your SIEM.

Why they ask

This tests whether you understand a real end-to-end investigation process rather than just naming tools.

How to structure your answer

Process walkthrough: describe each step in order, from initial triage through to containment and reporting, and note what evidence you'd gather at each stage.

Example answer

“I'd start by pulling the SIEM alert details to confirm the source host, destination, and volume of traffic involved. Next I'd check whether the destination IP has a known bad reputation using threat intelligence feeds, and cross-reference with firewall and DNS logs to see if this matches a known pattern like data exfiltration or command-and-control traffic. If it looks suspicious, I'd isolate the host from the network while preserving logs and memory for further analysis, then use Wireshark to inspect the actual packet captures if available. Once I've confirmed whether it's malicious, I'd document the timeline, the affected systems, and the remediation steps taken, and brief the relevant business unit if any data may have been exposed.”

2. You're midway through a scheduled penetration test when you discover a live, unpatched vulnerability that's actively being exploited by an external attacker. What do you do?

Why they ask

This checks judgement under pressure and whether you know when to stop testing and switch to incident response.

How to structure your answer

Judgement under pressure: state your immediate priority, explain the trade-offs you're weighing, and describe who you'd escalate to and when.

Example answer

“My first priority shifts from testing to incident response, since a live exploit takes precedence over the scheduled assessment. I'd pause the test immediately to avoid adding noise to the logs, then escalate to the incident response lead and relevant system owner with exactly what I've found: the vulnerability, evidence of active exploitation, and affected systems. Depending on severity, I'd recommend isolating the affected system while the team confirms scope. I'd keep detailed notes of what I observed and when, since that timeline matters for both the incident report and any regulatory notification obligations.”

3. Tell me about a time a business unit pushed back on a security recommendation you made.

Why they ask

This is a common friction point in the role, since security advice often adds cost or friction to business operations.

How to structure your answer

STAR: set out the situation, the specific action you took to address the pushback, and the outcome, focusing on how you balanced security risk against business needs.

Example answer

“A business unit wanted to keep a legacy application running without multi-factor authentication because it would slow down their workflow. I explained the specific risk in terms they cared about, including the potential cost and downtime of a credential compromise, rather than just citing policy. I then proposed a phased rollout of MFA on their least disruptive login points first, with a short trial period. They agreed to the trial, saw it caused minimal disruption, and rolled it out fully within the following weeks.”

4. How do you stay current with new vulnerabilities and threat actor techniques?

Why they ask

The threat environment changes constantly, and employers want evidence of an ongoing habit rather than a one-off certification.

How to structure your answer

Knowledge and approach: describe your regular sources and how you apply what you learn to your actual work, not just a list of things you read.

Example answer

“I follow ACSC advisories and vendor security bulletins relevant to the tools we run, and I check CVE databases against our asset inventory when a major vulnerability is disclosed. I also review post-incident writeups from other organisations when they're published, since they often reveal attack patterns worth checking for in our own logs. When something relevant comes up, I flag it to the team and check whether our current detection rules would actually catch it.”

5. How would you explain a critical vulnerability finding to a business manager with no technical background?

Why they ask

Analysts spend real time advising non-technical stakeholders, so this tests clarity and judgement about what detail matters.

How to structure your answer

Communication approach: describe how you'd frame the risk in business terms, what you'd leave out, and how you'd check they understood the ask.

Example answer

“I'd avoid technical jargon and focus on what the vulnerability means for their operations: for example, that an unpatched system could let an attacker access customer records, and what that would cost in downtime or reputational damage. I'd give them a clear recommendation with a timeframe, such as patching within a set window, and offer to answer follow-up questions. I'd also confirm they understood the urgency before ending the conversation, since a vague warning without a clear ask often gets deprioritised.”

6. What's your process for triaging results from a vulnerability scan across a large environment?

Why they ask

Scanners generate large volumes of findings, and employers want to know you can prioritise sensibly rather than treating every result as equally urgent.

How to structure your answer

Process walkthrough: explain how you sort and prioritise findings, and what factors push something up or down the list.

Example answer

“I start by filtering out false positives and duplicates, then prioritise based on a combination of severity score, whether the affected system is internet-facing, and whether there's a known exploit in the wild. A high-severity finding on an internal, isolated test server gets less urgency than a medium-severity finding on a public-facing server handling customer data. I then group related findings by system owner so remediation can be assigned efficiently, and I track progress against agreed patching timeframes rather than just closing the report and moving on.”