**Security Posture & Risk Assessment**

**Interview Questions**

The following set of questions has been prepared for the purpose of this interview. Some questions may require concise, one-sentence responses, while others may call for more detailed information. Please feel free to answer to the best of your ability. If any question involves sensitive or confidential information that you are not comfortable sharing, it is entirely acceptable to refrain from providing those details. However, we kindly encourage you to share as much relevant information as possible, as your insights are greatly valued.

**1. General IT & Security Questions**

• What security frameworks does your organization follow (e.g., NIST, ISO 27001, CIS Controls)?  
Our organization adheres to a hybrid approach by implementing ISO 27001 standards along with the Australian Cyber Security Centre’s (ACSC) Essential Eight strategies. ISO 27001 provides a comprehensive framework for establishing, implementing, and continuously improving an information security management system (ISMS). Meanwhile, the Essential Eight offers a prioritized set of baseline mitigation strategies tailored for Australian organizations, with maturity levels ranging from 1 to 8. This dual-framework approach helps ensure our information security controls are both globally recognized and locally relevant.

• How does your organization monitor and respond to security threats?  
We utilize a robust Security Information and Event Management (SIEM) system that collects and analyzes logs and security events from across our IT infrastructure in real-time. This system is integrated with our 24/7 Security Operations Centre (SOC), which actively monitors alerts, correlates threat intelligence, and coordinates incident response efforts. Any suspicious activity is immediately investigated and, if necessary, remediated following our established incident response protocols.

• What is the organization's approach to security awareness training?  
Security awareness is a core part of our organizational culture. All new employees undergo comprehensive security training as part of their onboarding process. This training covers a wide range of topics including phishing awareness, safe internet usage, and data protection best practices. Additionally, we conduct monthly refresher sessions and simulated phishing campaigns to continuously educate staff and test their ability to recognize and handle social engineering attacks.

**2. Shadow IT & Unauthorized Applications**

• How does the organization identify and track unauthorized IT resources (Shadow IT)?  
To manage the risks associated with Shadow IT, we implement advanced network monitoring tools and deploy Cloud Access Security Brokers (CASBs). These tools help detect and log all network activity, enabling us to identify unauthorized devices, applications, or services that may be accessing our systems. Through traffic analysis and anomaly detection, we can quickly pinpoint unapproved resources and take appropriate action.

• What policies are in place to regulate the use of third-party cloud applications?  
The use of third-party cloud applications is tightly governed under our Cloud Usage Policy. This policy requires all employees to seek formal approval before engaging with any external services. Requests are assessed for security, compliance, and data protection risks by our IT security team before being granted. This ensures all third-party applications align with our security standards and do not expose the organization to unnecessary risk.

**3. Network & Data Security**

• How is network traffic monitored for potential threats and anomalies?  
Our organization employs both Intrusion Detection and Prevention Systems (IDS/IPS) as well as behavior analytics tools to monitor network traffic. These systems detect patterns, anomalies, and potentially malicious activity by analyzing both signature-based and behavioral indicators. This layered monitoring approach allows us to proactively identify and neutralize threats before they can impact operations.

• What security measures are in place to protect critical data (encryption, backups, access control)?  
We enforce strict data protection protocols including end-to-end encryption for all critical data—both at rest and in transit. In addition, access to sensitive data is governed by Role-Based Access Control (RBAC), ensuring only authorized users can access specific information. Regular data backups are performed and stored securely to ensure data integrity and availability in case of a breach or system failure.

• How often are security audits and vulnerability assessments conducted?  
To maintain a strong security posture, we conduct vulnerability assessments on a quarterly basis. These assessments identify weaknesses and ensure timely remediation. In addition, annual penetration testing is performed by third-party security experts to simulate real-world attack scenarios and evaluate the effectiveness of our defenses.

• Are there any known vulnerabilities or security gaps in the organization's IT infrastructure?  
Currently, there are no critical vulnerabilities or unresolved security issues within our infrastructure. We maintain a proactive approach to vulnerability management, guided by a well-defined remediation process that prioritizes risk and ensures timely resolution.

• How is data classified based on sensitivity and protected accordingly?  
We follow a formal data classification policy that categorizes data based on its sensitivity and business value. Labels such as Public, Internal, Confidential, and Highly Confidential are applied, and security controls are tailored accordingly. This ensures that access, handling, and storage of data align with its classification level, providing appropriate levels of protection across all systems.

**4. Incident Response & Compliance**

* What is the organization's protocol for handling security incidents?
  + We have a formal incident response plan covering detection to post-incident review.
* How quickly can the organization detect and respond to a security breach?
  + We aim to detect threats within minutes and start remediation process once the breach has been patched.
* How is compliance with security standards ensured and documented?
  + We conduct internal audits and maintain documentation in our ISMS.

**5. Recommendations & Security Improvements**

* What is the biggest security challenging the organization currently faces?
  + Staying ahead of emerging threats and securing endpoints in hybrid work models.
* Are there any security enhancements planned for the near future?
  + Implementing Zero Trust Architecture, upgrading our IAM system and utilizing AI based detection and response systems.
* What additional security tools or practices would improve the organization's security posture?
  + Incorporating AI-driven threat detection, enhancing EDR and improving CSPM

**6. Remote Work & Mobile Device Security**

* Do employees work from home or use their phones/laptops for work?
  + Yes, employees use corporate-issues laptops and mobile devices.
* How do you keep remote devices safe from hackers or viruses?
  + Devices are secured with endpoint protection, MFA, MDM tools and conditional access policies.
* What happens if a work phone or laptop gets lost or stolen?
  + Devices can be remotely wiped, and an investigation is conducted.
* Are remote workers required to use VPNs or special security tools?
  + Yes, all remote employees are required to use VPN and MFA for secure access.

**7. Software & Patch Management**

* How do you ensure all software is up to date and secure?
  + We use patch management tools to automate updates and track compliance.
* How often do you review and update your software and operating systems?
  + Software updates are reviewed monthly, with critical and zero-day patches applied immediately.
* What happens if a critical patch needs to be applied quickly—how do you handle it?
  + We have a fast-track process and push emergency patches withing 24 hours.

**8. Firewall Configuration**

* What types of firewalls are deployed (stateful, next-gen, web application firewalls)?
  + We use next-generation firewalls, WAFs and traditional stateful firewalls.
* How are firewall rules audited and maintained for least privilege access?
  + Firewall rules are reviewed quarterly and follow the least privilege principle.