Table for Pros and Cons of the interview questions and answers.

|  |  |  |
| --- | --- | --- |
| **Category** | **Pros** | **Cons** |
| Security Frameworks | Clear dual-framework approach (ISO 27001 + ACSC Essential Eight)  Explains purpose and benefit of each | Could include maturity level achieved in Essential Eight for more depth |
| Security Awareness Training | Covers onboarding, monthly sessions, and phishing simulations | Could mention whether training effectiveness is measured |
| Third-party Applications | Approval-based system.  Assessed for risk and compliance | Could describe who evaluates and approves tools |
| Security Challenges | Highlights hybrid work and endpoint security as issues | Doesn’t explain how these are currently being managed |
| Firewall Rule Management | Reviewed quarterly.  Follows change management process | Could benefit from automation tools or more frequent review for dynamic environments |
| Critical Patch Handling | Fast-track process enables patching within 24 hours | Doesn’t mention rollback plan if patch causes issues. |
| Planned Enhancements | Mentions Zero Trust, IAM upgrades, and AI tools | Timeline for implementation not provided |
| Compliance Documentation | Stored in ISMS.  Ongoing internal audits | Could elaborate on external certification timelines |
| Incident Response | Covers full lifecycle from detection to recovery.  Includes post-incident reviews | Doesn’t mention team roles or communication strategies |
| Detection Speed | Real-time monitoring. Rapid containment emphasized | No specific metrics shared (e.g., mean time to detect/respond) |
| Vulnerability Status | Proactive management approach  No critical issues reported | Statement may seem overly optimistic without evidence |
|  |  |  |

Compare EDR solutions (e.g crowdstrike vs. Microsoft Defender) for cost, features and compatibility.

|  |  |  |
| --- | --- | --- |
| **Criteria** | **CrowdStrike Falcon** | **Microsoft Defender for Endpoint** |
| Cost | Premium price; billed per endpoint/year. Starts ~$8-16/month per endpoint depending on tier. | Often bundled with Microsoft 365 E5, so low extra cost if already using Microsoft ecosystem. Can be cheaper in Microsoft environments. |
| Deployment | 100% cloud-native. Lightweight agent, fast to deploy. | Cloud + on-prem hybrid support. Agent preinstalled on Windows 10/11. |
| Detection & Response | Strong AI-based behavioral analysis. Real-time detection with threat hunting (Falcon OverWatch). | Good integration with Defender ATP, Windows Event logs, and Microsoft Threat Intelligence. Advanced detection capabilities. |
| Insider Threat Detection | Has powerful behavioral analytics and identity protection, but better at external threats. | Strong insider threat detection due to integration with Azure AD, cloud apps, and behavioral data. |
| Threat Intelligence | Uses CrowdStrike Threat Graph and global intelligence from threat actors. | Integrated with Microsoft Threat Intelligence and Defender ecosystem. |
| Compatibility (OS) | Windows, macOS, Linux. Also supports mobile via CrowdStrike Mobile. | Strong with Windows. Also supports macOS, Android, iOS, Linux (less mature than Windows). |
| Integration | API-based integration with third-party SIEMs, firewalls, cloud tools. | Deep integration with Microsoft tools: 365, Azure, Intune, Sentinel, etc. |
| User Interface | Clean and modern dashboard. Easy for security teams. | Familiar interface for Microsoft users, integrated in Microsoft Security Portal. |
| Response Time | Fast alerts and automated response playbooks. | Strong automation with Microsoft Defender + Logic Apps/Power Automate. |
| Offline Protection | Good offline protection, relies on local behavior engine. | Uses cloud and local detection, but best when connected to cloud. |
| Use Case Suitability | Best for large enterprises with mixed environments and advanced threats. | Best for orgs using Microsoft 365 and Azure stack, especially mid-sized companies. |