convergent

Cloud, Hybrid and Application Security Professionals

www.convergentrisks.com

Examples of Typical Findings from a Cloud Security Assessment

Security Domain	Common Security Vulnerabilities
• Vulnerability Management	➢ No Vulnerability scanning tool in place for Virtual Machines
• Network Security	➢ Open permissive rules in place
• Network Security	➢ WAF not in place for web application security or rules are not aligned to OWASP Top10
• Anti-Malware	➢ No anti-malware in place for VMs or containers
• Key Management	➢ Keys and Secrets should be rotated regularly
• Pipeline	➢ No vulnerability scanning for CI/CD pipelines, lacking RBAC control
• Governance	➢ Lack of tooling in place to prevent security misconfigurations (e.g. Guardrails)
• Governance	➢ Lack of or no documentation in place for management, incident management, security monitoring, change management, secure development, vulnerability management, Hardening guidelines, workflow diagram etc.
• Data Protection	➢ Data is not protected in transit or at rest (no encryption)
• Secure Coding	➢ Vulnerability scanning of code not in place
• Databases	➢ No database security monitoring in place
• Personnel	➢ Lack of Security expertise within the organisation
• Security Monitoring	➢ Lack of active security monitoring for malicious behaviour and misconfigurations
• Identity & Access Management	➢ Lack of centralise identity and inconsistent application of MFA
• Security testing	➢ No penetration testing performed on the SaaS Platform