Executive Brief

We conducted a realistic red-team exercise simulating attackers from initial phishing to cloud data exfiltration. Attackers gained access via a credential-capture technique, escalated privileges due to overly-permissive cloud roles, and exfiltrated mock data from a public storage bucket. Key risks include weak cloud access controls, insufficient endpoint telemetry for fileless attacks, and reliance on password-based authentication. Recommended immediate actions: restrict cloud privileges to least-privilege, enable comprehensive cloud and endpoint logging, adopt phishing-resistant MFA, and run regular adversary-emulation drills. These steps will substantially reduce the risk of data loss and improve incident detection and response.