APJ SecureCloud – Incident Response Tabletop Exercise 2025

Scenario Summary:

A simulated incident involving suspicious privileged identity activity was executed to validate APJ SecureCloud's IR readiness across detection, analysis, containment, eradication, and recovery.

Timeline of Events:

• 09:12 – Sentinel correlates anomalous PIM elevation patterns (High Severity)

• 09:13 – Security Analyst validates Identity Protection risk signals

• 09:17 – Compromised user's session forcibly terminated; PIM elevation revoked

• 09:25 – Key Vault access logs analyzed for tampering or misuse

• 09:32 – Root Cause Analysis identifies credential theft as the entry vector

• 09:48 – Customer stakeholders notified with recommended mitigation steps

• 10:12 – Log ingestion validated; Sentinel baselines restored; incident closed

Lessons Learned:

• Enhance alert tuning for privileged role activation windows

• Increase MFA challenges for high-risk authentications

• Improve correlation between PIM, Key Vault, and Activity Log signals

• Expand runbook automation for session termination and token revocation

Outcomes:

• No customer metadata impacted

• Containment actions executed within required SLA windows

• IR runbooks updated with new steps for cloud identity compromise scenarios

• New Sentinel detection rule added: "Rapid PIM Elevation Abuse Detection"

This document serves as evidence for FedRAMP Low (LI-SaaS) IR-3 compliance.