Southern Mutual Bank

51 824 753 556

SOC Monitoring Report — Q3 2025

Report · synthetic assessor-grade test document

Generated 09 November 2026 · CyberSentien test harness · personalised to Southern Mutual Bank

Report ID	SOU-RPT-0207
Prepared by	Daniel Wright (Business Continuity Manager)
Classification	Internal Use Only
Status	Final
Reporting period	Q3 2025
Distribution	Control owner; Risk & Compliance; Internal Audit

1. Scope and method

This report records the results of soc monitoring report for Southern Mutual Bank over the reporting period. Results were produced from the system of record and the tooling named below; exceptions are listed with an owner and a due date and are tracked to closure by the control owner, with second-line oversight.

2. Summary of results

Security events ingested into the SIEM	1.2 billion — event logs, audit logs, network and identity sources; log retention 12 months
Alerts triaged (security monitoring, intrusion detection, anomaly detection)	3,418
Alerts triaged within SLA	97.8% — alerting reviewed by the 24x7 security operations centre
Escalated to security incident	6 — continuous monitoring use cases reviewed monthly

3. Results

Detection use case	Alerts	Triaged within SLA	Escalated	Log source	Analyst lead
Data exfiltration alert	234	96%	1	Identity provider sign-in log	Aisha Khan
Privileged account anomaly	53	97%	3	DLP	Laura Mendez
Privileged account anomaly	226	98%	4	EDR telemetry	Daniel Wright
Privileged account anomaly	164	100%	4	SIEM correlation rule	Nadia Petrova
Data exfiltration alert	168	96%	4	SIEM correlation rule	Greg Thompson
Impossible travel sign-in	37	95%	2	EDR telemetry	Mei-Lin Tan

Detection use case	Alerts	Triaged within SLA	Escalated	Log source	Analyst lead
Data exfiltration alert	47	97%	1	EDR telemetry	Priya Sharma
Data exfiltration alert	211	90%	3	DLP	James O'Connor
Malware detected by EDR	202	97%	0	DLP	David Okafor
Privileged account anomaly	54	91%	3	Identity provider sign-in log	Tom Bauer

4. Findings and follow-up actions

No exceptions were identified in the period.

5. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification

6. Review and approval

Role	Name	Date
Prepared by	Daniel Wright	03 Nov 2026
Reviewed by (2nd line)	Mei-Lin Tan	06 Nov 2026
Approved by	Chief Information Security Officer	08 Nov 2026