**Fraud & Security Incident Reports with Response Actions**

These reports focus on unauthorized access attempts, breaches, and fraud patterns.

**Contents:**

* **Security Events:** Summary of suspicious activities, login anomalies, privilege escalations.
* **Fraud Detection Logs:** Cases flagged by fraud detection rules (e.g., duplicate transactions, threshold breaches).
* **Incident Response Timeline:** Detection time, response action, recovery time.
* **Root Cause Analysis:** Post-mortem of the incident.
* **Preventive Actions:** Policies or patches deployed after the incident (e.g., updated IAM roles, new firewall rules).

**Tools Used:** AWS GuardDuty, SIEM tools (e.g., Splunk, IBM QRadar), Odoo’s Audit Logs, Suricata, OSSEC  
**Purpose:** Ensure data integrity, legal compliance (e.g., GDPR, ISO 27001), and bolster trust with users.