A Telco-aware SIEM Pipeline for Real-time Endpoint, Cell Behavior, Kernel Analysis, and Fraud Detection

Tri Sumarno, S.H M.T.I
tri@noz.co.id

Abstract. Modern telecommunication networks have evolved into complex cyber–physical systems where security monitoring requires deep awareness of signaling, endpoint behavior, and network kernel activity. Conventional Security Information and Event Management (SIEM) solutions are primarily designed for IT infrastructures, lacking contextual understanding of telecom protocols, radio events, and signaling behavior defined by 3GPP. As a result, they fail to provide early detection of anomalies and fraud within cellular environments.

This research introduces SIEM Telco, an open-source and telco-aware SIEM framework that integrates signaling intelligence, kernel telemetry, and behavioral analytics into a unified real-time detection pipeline. The system collects and correlates multi-layer telemetry from radio access (OpenBTS, Osmocom), network behavior (Ella-core), and host-level kernel logs to detect anomalies that traditional IT-oriented SIEM overlook. Through a modular pipeline, SIEM Telco enables cross-layer correlation between signaling messages (e.g., Paging Request, Attach Request, Location Update), cell activity, and endpoint interaction to identify abnormal patterns such as fraudulent IMSI usage, rogue base stations, and signaling-based denial-of-service attempts.

The proposed architecture adopts a hybrid approach combining stream-based analytics and rule-based correlation to balance latency and accuracy. Initial evaluations on an emulated GSM/LTE environment demonstrate that SIEM Telco achieves near-real-time anomaly detection (<200 ms per event) with a 93% detection accuracy and reduced false positives by 37% compared to a baseline ELK-based SIEM. The results confirm that telco-aware contextual correlation significantly enhances visibility, enabling operators to detect both cyber and signaling-layer threats before they escalate.

This paper contributes a replicable architecture, open dataset, and integration methodology bridging open-source telecom stacks with security analytics. Future work will extend SIEM Telco toward 5G core environments and integrate AI-driven correlation models to adapt dynamically to evolving telecom threat landscapes

Keywords: Telco-aware SIEM, Telecom Security, Signaling Analysis, Fraud Detection, 3GPP, OpenBTS, Osmocom, Real-time Monitoring, Behavior Analytics, Kernel Telemetry, Network Anomaly Detection, Open Source Framework, Cellular Network Security