Contribution ID: **252** Type: **Paper presentation**

Behavior Analytics for Centralized SIEM with Edge Processing

Thursday 18 September 2025 16:15 (15 minutes)

This paper proposes an integrated behavioral analytics framework that leverages the usage of a centralized SIEM, edge AI processing, and automation to enable adaptive, real-time detection and response.
By collecting diverse behavioral data: API calls of applications, system commands, authentication attempts, and web request patterns, using Wazuh agents from mixed environments, the system captures the operational fingerprint of an organization. AI models, are then trained on this data, allowing detection mechanisms to adapt dynamically to identify anormal behavior with high accuracy.
To achieve low-latency, models were developed and deployed on an NVIDIA Jetson Orin device at the network edge, removing cloud dependency while ensuring privacy and speed. Upon detection of suspicious activity, response actions are executed. This architecture, built with open-source technologies, demonstrates a scalable and modular system.
Experimental results show effective detection SQL injection attempts, and API-level anomalies, validating the system's potential for practical deployment in modern security operations.

Authors: Mr PETER, Cristian ("Transilvania" University of Brasov, Romania); Prof. BALAN, Titus ("Transilvania" University of Brasov); Mr CHIS, Alexandru ("Transilvania" University of Brasov)

Co-author: Mr DINU, Vladut Ionut ("Transilvania" University of Brasov)

Presenter: Mr CHIS, Alexandru ("Transilvania" University of Brasov)

Session Classification: Security & Resilience in Cyber-Physical Systems

Track Classification: Networking in Education and Research