Contribution ID: **79** Type: **not specified**

Network Automation for Intrusion Detection System

Wednesday, October 18, 2017 4:50 PM (25 minutes)

CERN networks are dealing with an ever-increasing volume of network traffic. The traffic leaving and entering CERN must be precisely monitored and analysed to properly protect the networks from potential security breaches. To provide the required monitoring capabilities, the Computer Security team and the Networking team at CERN have joined efforts in designing and deploying a scalable Intrusion Detection System (IDS). The initial setup, presented at the HEPiX Fall 2016 Workshop in Berkeley, featured a Brocade MLXe configured with OpenFlow to provide dynamic offload and selecting mirroring capabilities. Due to technical requirements, the setup has been evolved and currently leverages the Brocade SLX platform with network automation software (StackStorm / Brocade Workflow Composer) deployed for additional programmability and flexibility. The new technology stack is under testing with a promising perspective of production deployment in 2018.

Desired length

20

Primary author: KRAJEWSKI, Adam Lukasz (CERN)

Co-authors: STANCU, Stefan Nicolae (CERN); VALSAN, Liviu (CERN)

Presenter: KRAJEWSKI, Adam Lukasz (CERN)

Session Classification: Networking and security

Track Classification: Security & Networking