Contribution ID: **48** Type: **Oral**

Arhuaco: Deep Learning and Isolation Based Intrusion Detection in High Energy Physics

Thursday 24 October 2019 15:50 (20 minutes)

High Energy Physics utilizes powerful distributed computational networks called grids, to process and analyze scientific data. Monitoring the security of these networks is a challenging task. Arbitrary and not-trusted applications can be executed inside the grid worker nodes by the scientists. Innovative methods and tools are required to reduce the risk associated with the
execution of users' software (also called jobs), to identify cyber-security incidents and to perform autonomous responses. The isolation and monitoring of job payload activity are necessary in order to protect the computational infrastructure and to find evidence of malicious behavior. We describe a security architecture that integrates Linux containers to safely execute grid jobs with behavior monitoring powered by deep learning methods for the analysis of real-time data to detect and prevent intrusions. A generative method with recurrent neural networks is utilized to improve the detection performance. We describe how these methods aim to increase the security of computational grids, improving existing solutions. We present Arhuaco, a proof-of-concept implementation and provide an evaluation for the ALICE collaboration grid at CERN.

Primary author: GOMEZ RAMIREZ, Andres (Johann-Wolfgang-Goethe Univ. (DE))

Co-author: KEBSCHULL, Udo Wolfgang (Johann-Wolfgang-Goethe Univ. (DE))

Presenter: GOMEZ RAMIREZ, Andres (Johann-Wolfgang-Goethe Univ. (DE))

Session Classification: Submitted contributions

Track Classification: Societal challenges