Contribution ID: **252** Type: **Poster**

A Security Monitoring Framework For Container Based HEP Computing Infrastructures

Tuesday 11 October 2016 16:30 (15 minutes)

Distributed computing infrastructures require automatic tools to strengthen, monitor and analyze the security behavior of computing devices. These tools should inspect monitoring data such as resource usage, log entries, traces and even processes' system calls. They also should detect anomalies that could indicate the presence of a cyber-attack. Besides, they should react to attacks without administrator intervention, depending on custom configuration parameters. We describe the development of a novel framework that implements these requirements for HEP systems. It is based on Linux container technologies. A previously unexplored deployment of Kubernetes on top of Mesos as Grid site container based batch system, and Heapster as a monitoring solution are being utilized. We show how we achieve a fully virtualized environment that improves the security by isolating services and jobs without an appreciable performance impact. We also describe an novel benchmark dataset for Machine Learning based Intrusion Prevention and Detection Systems on Grid computing. This dataset is built upon resource consumption, logs, and system call data collected from jobs running in a test site that has been developed for the ALICE Grid at CERN as a described framework's proof of concept. Further, we will use this dataset to develop a Machine Learning module that will be integrated with the framework, performing the autonomous Intrusion Detection task.

Tertiary Keyword (Optional)

Cloud technologies

Secondary Keyword (Optional)

Artificial intelligence/Machine learning

Primary Keyword (Mandatory)

Security and policies

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

Co-authors: Dr LARA, Camilo (Johann-Wolfgang-Goethe Univ. (DE)); Prof. KEBSCHULL, Udo Wolfgang (Johann-Wolfgang-Goethe Univ. (DE))

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

Session Classification: Posters A / Break

Track Classification: Track 8: Security, Policy and Outreach