Contribution ID: **136** Type: **Invited talk (plenary/keynote)**

Testing and Training Cybersecurity using a virtual platform

Tuesday, 5 December 2017 13:30 (30 minutes)

Cybercrime and cyber vulnerabilities are increasing both in number and complexity and pressure is on business and industry to employ cybersecurity professionals that are able to defend systems and infrastructure against cyber-attacks. As a country's critical infrastructure can be exposed through integration of IoT and Smart Cities, the need has been identified to develop a platform to conduct various tests focusing on securing the implementations before deployment. The platform provides a virtualised space for the simulation or emulation of enterprise networks to conduct various forms of testing as well as the training of cybersecurity specialists. This hyper-realistic simulation virtual training environment normally resembles the enterprise network or operational environments where the cyber workforce can do using red and blue team exercises that can develop their skills to defend their company networks. Doing training on these platform offer the opportunity for a cyber team to work together, as one team, across multiple security domains to defend their networks, reinforcing the skills and opportunity for shared security responsibility for the company, agency or service. In addition it improve their ability to identify advanced attacks.
The Network Emulation and Simulation Laboratory (NESL) at the CSIR, is developed to support higher education and industry to perform network bandwidth and performance modelling, cybersecurity training, device research and advanced analytics to study cyber risks and to deliver effective and practical security solutions, all within the safety of an isolated environment. This platform can also be used to do quantitative, qualitative and realistic assessment of potentially ground-breaking cyber technologies for research and development. It also includes hardware in the loop and malware capability for the emulation of real attacks.

HPC content

HPC can be used to support the NESL platform by conducting big data analysis of various cybersecurity attacks which includes but is not limited to malware and DDOS attacks. The HPC capability can be used for the investigation and impact analysis of malware as part of an use case (exercise) in NESL

Primary author: Prof. JANSEN VAN VUUREN, Joey (CSIR)

Co-author: Mr LABUSCHAGNE, Aubrey (CSIR)

Presenters: Mr LABUSCHAGNE, Aubrey (CSIR); Prof. JANSEN VAN VUUREN, Joey (CSIR)

Session Classification: SA NREN

Track Classification: SA NREN