

Risto Vaarandi

In March 9-12 2015, senior researcher Risto Vaarandi from Tallinn University of Technology participated in the IEEE CogSIMA 2015 conference, in order to present the poster paper “Simple Event Correlator – Best Practices for Creating Scalable Configurations” (coauthored by Bernhards Blumbergs and Emin Caliskan). IEEE CogSIMA is an annual conference which focuses on situational awareness and situation management issues. Simple Event Correlator that is presented in the paper is a tool that has been adopted for event correlation by a number of large organizations, and is helping to improve situational awareness in telecom companies, banks and other financial institutions, universities and research labs, supercomputing centers, military and government organizations, and various other institutions. The paper describes various techniques of creating scalable configurations for the most recent major release (2.7.X) of Simple Event Correlator, and presents a number of event correlation rule examples for processing security events. The paper (5 pages) has been included in electronic conference proceedings and will also be published by IEEEExplore.

