SEC - Simple Event Correlator Evaluation Public Report

25 April 2014

An evaluation of the SEC (version 4.0.1) for event correlation was performed by the Technology Investigation Service evaluation team. Event correlation is a procedure where a stream of events is processed in order to detect and act on certain event groups that occur within predefined time windows. The effectiveness of an event correlator is the range of actions which can be automated upon the detection of a specified event.

This lightweight and platform-independent event correlation tool allows users to cause an action to be performed in the case of single or multiple events that are correlated. The actions can be simple log messages, email alerts or execution of scripts. The events can be correlated by time or pattern matching from a variety of log sources or other real time inputs.

SEC was tested for a variety of event correlation use cases. These included monitoring, reporting and executing actions on an nfs server, ssh server, Genesis II job execution server, and log rotation with Yum. The tests chosen for this evaluation highlight a wide variety of event correlation tasks such as log-file analysis, machine state operations, logic analysis and more. In all cases, SEC performed as expected. We also tested a number of simple error conditions, to which SEC provided appropriate and informative error messages.

SEC is a versatile tool and its strength is that it can monitor a wide variety of applications including basic operating system related applications, applications that rely on OS monitoring, other applications or advanced systems and can be configured to intelligently respond to certain situations. SEC can also to used to monitor multiple applications on same machine at the same time. Additionally, it is easy to install and configure, save for the difficulties of writing regular expressions. System administrators or anyone interested in monitoring applications with logs will find it useful.

We recommend SEC for event correlation.