SNORT Plus

SNORT Plus – is a Multi-Level Evidence Based Intrusion Detection System Using Bayesian Network to Detect Insider Threats. The insider threat is one of the most insidious and difficult threats to catch to cyber security specialists and network defenders. To facilitate early and accurate detection of the insider threat, a number of new methods and ideas should be explored. First, there must be a technique to understand the behavior of information system users and to be able to determine that a user's behavior is not normal. There must be ways to accurately model human behavior against stated security policies. Current intrusion detection systems (IDS) perform poorly in detecting new or previously unseen attacks. They are generally designed to detect (and possibly block) conventional, external, network-based threats. The IDSs might require extensive modification to the rule sets to detect the insider threat. Our modeling on insider threat detection using Netica will be plugged-in to Snort IDS as a preprocessor. Snort is a modern security application with three main functions: it can serve as a packet sniffer, a packet logger, or a network-based IDS. There are also many add-on programs to Snort to provide different ways of recording and managing Snort log files, fetching and maintaining current Snort rule sets, and alerting to let system administrators know when potentially malicious traffic has been seen. – Sheldon/Yoo (UofAL)/Ferragut.

POC: Frederick Sheldon, PhD, Michael Neergaard, MS; Erik Ferragut, PhD
Cyberspace Sciences & Information Intelligence Research (CSIIR) Group
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418
www.ioc.ornl.gov