

Haystax presents: Advanced Analytic Techniques for Insider Threat Detection

Insiders are one of the top categories of data breaches according to recent reports by the FBI, Forrester Research and Verizon. In just the last year, high profile data breaches at Target, AT&T, and Morgan Stanley show that no organization is immune and all organizations must take steps to identify and protect themselves from insider threats.

In this webinar Haystax describes an analytic approach that enables the continuous risk monitoring of insider threat based on the fusion of high and low frequency entity-related events via temporal relevance models and a probabilistic risk model. Haystax begins by providing an overview of their approach and the challenges faced when integrating events of widely disparate frequency. Next, they describe two forms of event temporal relevance they use to enable the model to fuse infrequent events (e.g. public records life events) with high frequency events (e.g. network activity). Finally, Haystax describes how they've used Franz's Allegro Common Lisp, Allegro Prolog, and AllegroGraph, with Norsys Metica to create a practical implementation of our analytic approach suitable for practical use.

The webcast noted above is a complimentary presentation to Haystax's paper presented at STIDS (Semantic Technology for Intelligence, Defense, and Security).

Download the [STIDS](#) paper

Download the [STIDS](#) presentation

View a recording of this webcast [here](#)

Download the webcast presentation slides [here](#)