Thursday, February 17, 2022
10:30 AM – 10:50 AM
Threat Predict

Jason Weaver
Chief Solutions Officer
SkyePoint Decisions, Inc.

Abstract:
SkyePoint Decisions, Inc. (SkyePoint) and TIBCO Software Federal Inc. (TIBCO) introduced a use case application of the AI/ML capabilities of TIBCO Spotfire® to address cybersecurity challenges identified and discussed by Federal Agency cybersecurity leadership and management.

The outcome of SkyePoint's cybersecurity, network, and IT Infrastructure experience with the leading-edge capability of TIBCO Spotfire®, known as Threat Predict, is enhanced, informed, and predictive decision making for Agencies to meet unique cybersecurity challenges head-on. Threat Predict leverages AI/ML to identify and prevent known and unknown threats to enterprise networks by ingesting and visualizing data provided from traditional security sources like the SIEM and a multitude of other sources that provide enhanced context for information processing and analytics. By using both unsupervised and supervised ML models, natural language processing, predictive analytics capabilities, and AI, Agencies can increase the volume of data without further overwhelming cyber analysts while enabling the identification of new TTPs.

Increasing the volume and type of data monitored provides additional context to the cyber analyst while also empowering the analyst to focus their analytical skills on the critical cybersecurity operations problem sets to protect the network. Threat Predict serves as a force multiplier for security teams and enables analysts to get out in front of cybersecurity threats by offering better data and intelligence for use in cyber events and incident response.

The Threat Predict solution includes:

(1) Proactively Identifies Cybersecurity Anomalies providing actionable intelligence for SOC/NOC/CSIRC/NOSC/etc. analysts and cyber threat hunters to reduce risk and provide visibility to leadership.

(2) Leverages TIBCO's AI/ML and behavior recognition solution empowering agency cybersecurity management to get ahead of potential incidents.

(3) Delivers the missing context to what is happening on the network pointing analysts in the right direction and empowering collaboration between cyber teams, network teams, and informing leaders to make data driven decisions.