DRAGON SPEAR

POWERED BY
Business Integra

As threats evolve, and the methods used by threat actors become more sophisticated, there is a need to focus on the principles of data science to influence the development of new technologies and methods to better prepare against the very real and potential threats posed by these threat actors.

To establish a strong Cyber Threat Intelligence (CTI) program, the collection and analysis of extensive data is required. Due to the very nature of CTI and sandboxing, vast amounts of data are collected for analysis. However, due to the volume of data collected, it becomes impossible to manually review all low priority events, due to limited staff resources that are already overwhelmed with the number of findings, the majority of which are false alerts.

This situation leaves the real possibility that a true, high-value threat goes undiscovered, which could cause a massive security event that would impact operations.

Protect the Castle with DragonSpear

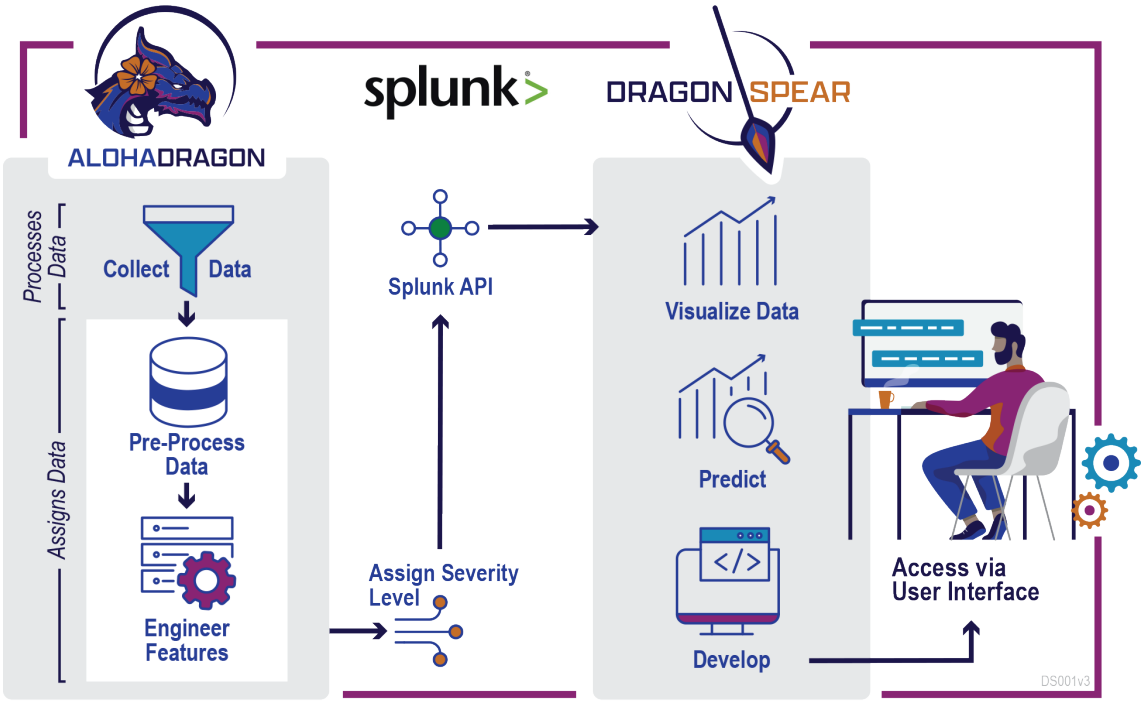
Business Integra (BI) and partner, Federal.ai, have produced an Artificial Intelligence (AI)/Machine Learning (ML) model-based product, called the ***DragonSpear Classifier***, *shown in Figure 1*, which is part of BI's leading-edge Dragon product suite.

The ***DragonSpear Classifier*** was designed to aid in the management of cybersecurity events, as an augmentation of SIEM strategies to correctly identify threats while preventing "alert fatigue" though Deep Learning enabled predictive analytics.

ALOHADRAGON

DRAGONMAGE

DRAGON SPEAR



(U) Figure 1: *DragonSpear Classifier*

DragonSpear Classifier Build Details

- Development of Custom Models
- Training and Unsupervised Learning
- Bayesian Probability Analytics and Advanced Research.

Build Components

Data Sources that contain diverse and legacy sources

Machine Learning to Identify and Track Threat Actors

AI to promote the to promote the reduction of information overload and Splunk API as a key data input stream to support the AI processes.

PRODUCT FEATURES

- **Built on the TensorFlow framework** for use with machine learning, deep learning, and other statistical and predictive analytics.
- **Lowers the chance of missing events** that appear to be low priority but will become critical over time – *without creating SIEM overhead.*
- Available to run on the Cloud, on-prem or in the ***DragonMage Appliance.***
- **Can ingest and be trained on a variety of data sets,** with a support infrastructure to assist in ingesting and training.
- **Runs outside of Splunk environment and does not add to the volume of processed data,** resulting in a more efficient use of SIEM.
- **Delivered with a Jupyter Notebook interface and analytics.**

CONTACT Fred Brott
VP National Security Group, BI
Fred.Brott@businessintegra.com
(o) 301.474.9600x177
(c) 469.586.6837