ResponSight

Corvum Analytics Engine

Data science and artificial intelligence for enhanced risk visibility

The Corvum analytics engine uses data science and artificial intelligence technologies to provide the risk measurement and anomaly detection capabilities of ResponSight's Corvum Suite. Through the incorporation of disparate sources of data collected at the endpoint, Corvum learns complex patterns of machine activity and user behaviour, from single-endpoints and across the enterprise. Following deployment, Corvum rapidly learns to identify main sources of risk, categorized by risk type, endpoint, and department, providing unparalleled visibility into the risk makeup of your organization and the tools to more accurately map the road to enhanced security.

Applications

- **Risk quantification**
- **Future risk modelling**
- **Risk & technology integration**
- **Better resource usage**
- **Decision support**

Features

- ✓ **Real-time adaption:** Corvum is an online learning system, meaning that it learns the features specific to your organisation and continuously improves in real-time as new information is collected.
- ✓ **Responsive:** changes in the risk structure of an organisation, introduced by external (unwanted) influences or by deliberate changes to the security infrastructure, can be assessed in real-time via changes in measured enterprise risk.
- ✓ **Fast returns:** clients will typically see informative enterprise and endpoint risk profiles within a week of deployment.
- ✓ **Extends existing technology:** this technology complements existing commonly used systems (e.g., SIEM) by prioritising detected threats using risk and escalating the priority of potentially dangerous but previously known threats.
- ✓ **Privacy-preserving:** analytics performed do not require access to sensitive, identifying, or personal data, without any loss of statistical power or accuracy.

Core algorithms

Predictive modelling for anomaly detection

Predictive algorithms are trained to encode information present in historical data enabling approximation of key activity and behavioural indicators. Corvum uses neural network and gradient-boosting machine algorithms to capture complex, nonlinear relationships in collected endpoint data. These learned relationships describe aspects of the historical, or normal, dependencies within the data, and can be used to predict movements in key metrics.

To identify anomalous activity on a machine or within an organization, series of predictive models can be used, where predictive error corresponds to deviations from typical activity, regardless of the cause of the deviation.

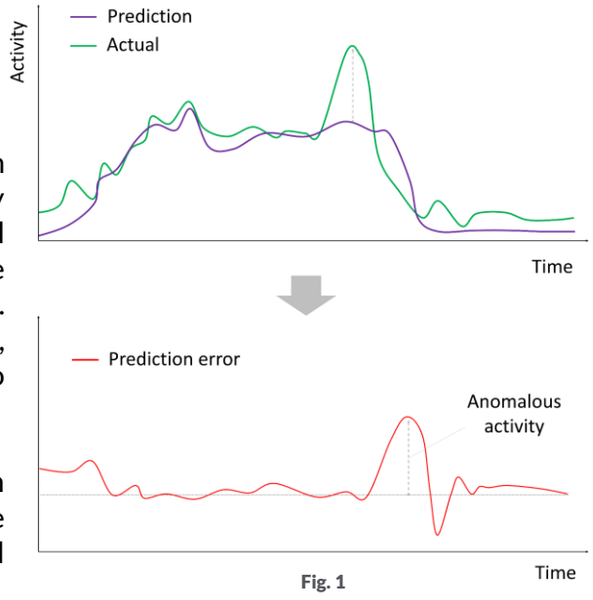

Fig. 1

ResponSight

CORVUM ANALYTICS ENGINE

Deep learning

If an attacker or malicious entity gains access, either physically or remotely, to a computer within an organization, it is crucial that the change in behaviour on that endpoint be observed and identified by monitoring systems. To detect a single machine being compromised, we need a model of normal for every computer and user. In general, this problem is intractable due to the large number of distinct endpoints with unique patterns of behaviour, making it easy for an attack to be hidden in the noise.

Drawing on cutting-edge techniques in AI for computer vision and facial recognition, Corvum uses deep learning models to encode and monitor the activity of arbitrary numbers of individual endpoints across the organization (see fig. 2). In application to Cybersecurity, facial image data is replaced with a wide set of user and machine activity. By learning to map incoming data accurately, activity for specific machines and groups of machines are clustered. When abnormal activity occurs on a machine, deep learning encodings deviate rapidly from the normal cluster and an anomaly is flagged. Deep learning models employed by Corvum update in a fully online manner, allowing for both real-time learning given up-to-date data and real-time recognition and risk measurement.

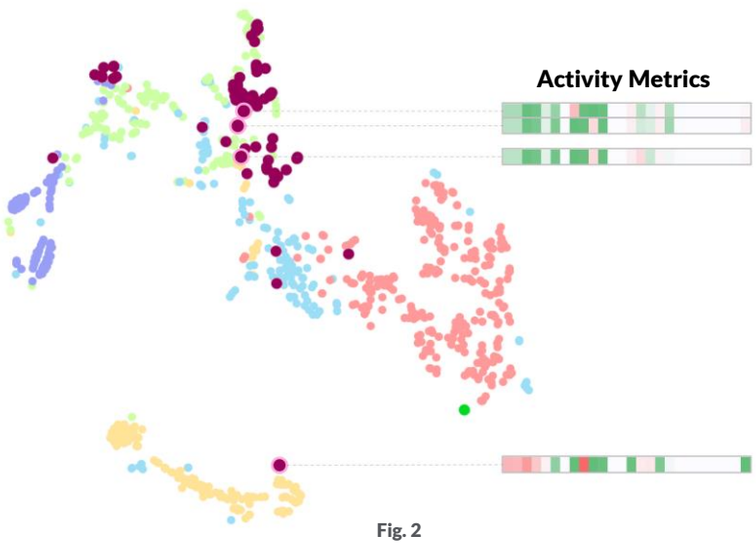

Fig. 2

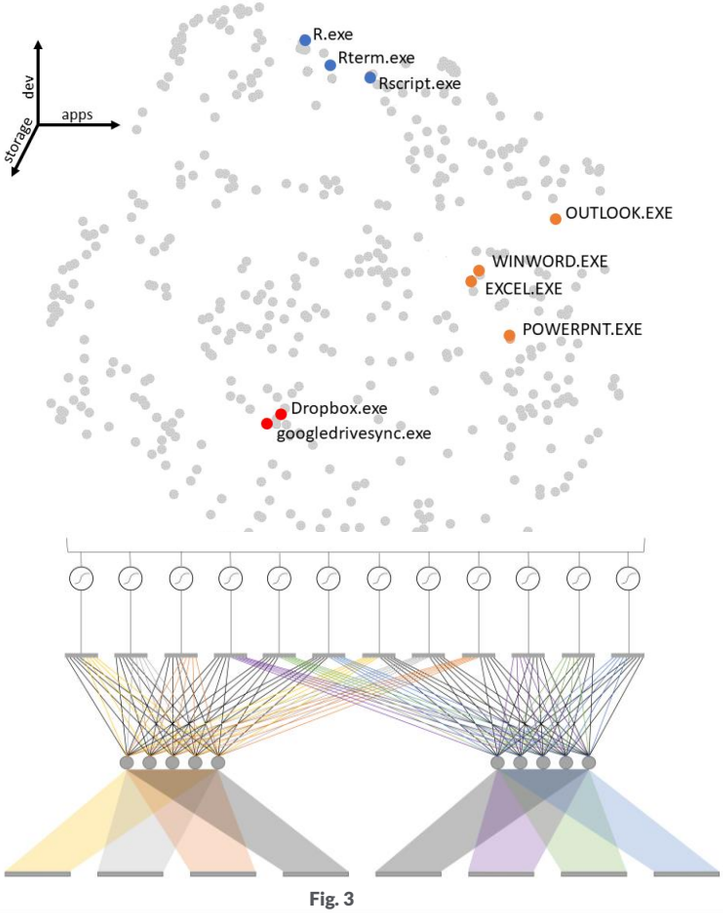

Fig. 3

Word embeddings and privacy-preserving analytics

Many sources of rich categorical endpoint data, such as process names, paths, IDs etc., are valuable information when read by a human. However, these data are not easily interpreted by algorithms, making it challenging to incorporate them into a sophisticated cyber solution.

Word embeddings, originally developed for Natural Language Processing, enable machine learning models to interpret the meaning and relationships between text-based categorical data. Corvum uses carefully tuned neural networks to learn to understand the common contexts and applications of various programs and files, embedding them into an abstract space representing specific and useful characteristics (see left).

In addition to the interpretive power of embeddings, they do not require that input data be human-readable and can be fully obfuscated and anonymized. ResponSight requires no sensitive information be sent outside of the client organization.

For more information, see our white paper, Data Science and AI Solutions for Cybersecurity, and our Corvum suite overview datasheet, available on www.ResponSight.com.

W: responsight.com **E:** info@responsight.com responsight