CS-AWARE
NEWSLETTER

INSIDE THIS ISSUE

By Peracton Ltd Ireland and Rheasoft Denmark

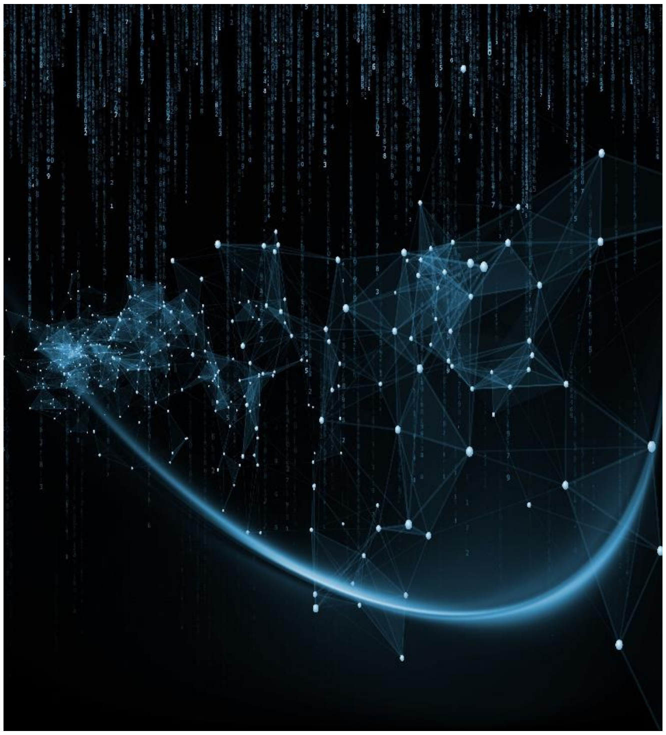
May 30, 2020

CYBERSECURITY DATA ANALYSIS

A LOCAL PUBLIC ADMINISTRATION APPLICATION BY PERACTON AND RHEASOFT

Our CS-AWARE project (https://cs-aware.eu/) is a H2020 funded EU project with a 3 years duration that now is towards its end (by August 2020). It has delivered a functional and demonstrable cybersecurity solution. From the very beginning, it focused on awareness and early threat detection. The solution was implemented at two pilot sites, namely the municipality of Larissa in Greece and Roma Capitale, Italy.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740723. This communication reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.



APPROACH

DECIDING ON SUSPICIOUS DATA EVENTS

At the core of our approach sits the data analysis component that is critical for processing all the internal and external data it receives for detecting threats. When a threat is detected, the visualisation component shows the threats to system administrators who can then easily handle them and raise the level of cybersecurity awareness internally. The data analysis component is powered by a proprietary big data analytics solution provided by Peracton Ireland and the visualisation is developed by Rheasoft, Denmark. There are two main data source: internal/private LPA data and public data, coming from online cybersecurity public forums / selected social media channels. The data first is pre-processed and then lifted to STIX2.0. Then the outcome is taken by the data analysis component and processed based upon the specific cyber security patterns we have designed for each pilot.

SOLUTION

TAYLORED CYBERSECURITY PATTERNS

The uniqueness and novelty of our data analysis approach is that we tailor it in an easy manner by designing and searching for very specific patterns, relevant for each LPA (Local Public Administration): some LPAs may have different focuses and different constraints, as well as different vulnerabilities in terms of their procedures, processes and technology stack. Thus our search is not a global one for random, potentially suspicious events, but targeted and narrowed down to the business processes and specific IT /security set-up, while still represented in an intuitive way for system administrators to grasp the situation and act fast on any threat detected.

THE CHALLENGES

CUSTOMIZED IMPLEMENTATION

One of the main challenges is first understanding the specific processes of an LPA that can vary widely given departmental scope, LPA size and organizational structure with different combinations of technologies involved. Once the processes are understood, a map of the LPA's components is drawn up in the visualisation frontend, and the patterns to be searched for are defined in the data analysis component. LPA unique cyber-security factors have to be defined and taken into account when looking for vulnerabilities while doing this. However,using the map and the knowledge of the LPA, it is possible to ensure that all corners have been searched.

RESULTS AND FUTURE WORK

All our tests have successfully passed the two LPAs data analysis, having two very different implementations and sets of results. However, in each case, threats are detected by the data analysis and presented in useful ways for the system administrator. As the project draws to a close at the end of August, future work in the cyber security data analysis started by us will be continued by the commercialization initiatives of the CS-AWARE project. This will involve a future increase of automation of data analysis, simpler cybersecurity requirements capture as well as faster implementation cycles for LPAs.