Cybersecurity Data Collection

By 3rdPlace Srl and University of Vienna

May 30, 2020

COLLECTING DATA LOGS FOR LOCAL PUBLIC ADMINISTRATIONS AND PUBLIC EXTERNAL DATA ABOUT POTENTIAL CYBER THREATS

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.

Inside this Issue

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.

COLLECT

FIND THE INFORMATION YOU NEED

We think the design of this newsletter is great as is! But, if you do not agree, you are able to make it yours by making a few minor design tweaks! Tips on updating specific features are available throughout this example text.

To change any of the text in this document, just click on the block of text you want to update! The formatting has already been programmed for ease of formatting.
You can easily change the overall colors of the template with just a few clicks. Go to the Design tab and click on Colors. From the list of colors, you can choose a different color scheme. As you hover over the different choices, you can see what the overall feel of the document will change with each different option.

UNDERSTAND

KNOW YOUR SYSTEM

To create a successful working solution, it is first necessary to study and understand the full system in place in the municipality. This involves knowing the various nodes composing their network, how they interact, and which technologies they use to implement their services. The second step is to understand what type of information we can extract from each node we want to monitor and how to correctly interpret the data.

For these reasons, in order to obtain a reliable solution, it is crucial to gather detailed information directly from the municipality about how their systems are expected to work and study the meaning of the data available. In this context, the CS-AWARE project has created a socio-technical system and dependency analysis approach, that includes the identification and analysis of relevant log files. This process aims to understand the relevance and meaning of individual log file parameters that are important to monitor specific security aspects.

Based on this in-depth understanding of the data produced by the identified log files, the actual collection and preprocessing can proceed. Nodes can usually be monitored by the periodic extraction and analysis of the data logs they produce. To achieve this result, log files are periodically extracted and pre-processed to match a common format we defined. In detail, as we follow the STIX 2.0 specifications to exchange messages within the system, all log files are converted to STIX 2.0 format and delivered to the analysis component that will then perform the analysis and data correlation aspects that CS-AWARE provides.

FLEXIBILITY

EXTENSION AND MAINTENANCE

This approach gives us the ability to support many different types of sources by abstracting from the original format. To support a new type of log file, all we need to implement is a custom adapter able to read the original data and convert it to STIX 2.0.

Particular attention is given to users' privacy to comply with GDPR regulation. A data anonymization process is provided by the CS-AWARE log collector. A Privacy Impact Assessment (PIA) needs to be conducted by each municipality. For data entries that represent personal data, that are in general security relevant (like IP address log entries), the municipalities need to decide during the PIA if those entries should be processed or removed by CS-AWARE, and if the processing can be done in clear or anonymized form. Personal data that is not security relevant is usually anonymized or completely removed from the processed logs.

We also focused on flexibility, supporting different types of storage for our data. Based on the necessities of the specific municipality, we are able to support both Cloud or on-premises deployment.