CS-AWARE
NEWSLETTER

## INSIDE THIS ISSUE

By InnoSec P.C. Greece and OTS S.A. Greece

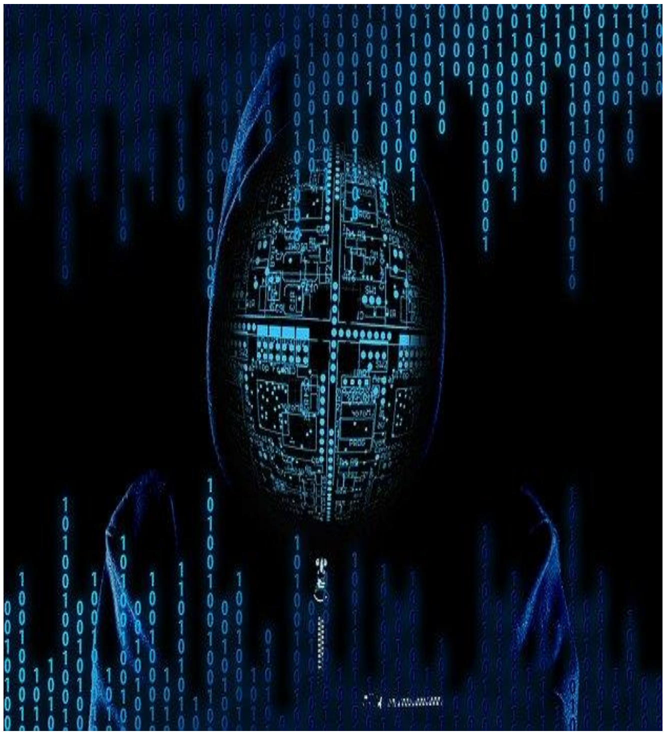
Jul 7, 2020

# SELF-HEALING IN CYBERSECURITY

A LOCAL PUBLIC ADMINISTRATION APPLICATION BY INNOSEC AND OTS

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, Greece and Roma Capitale, Italy.

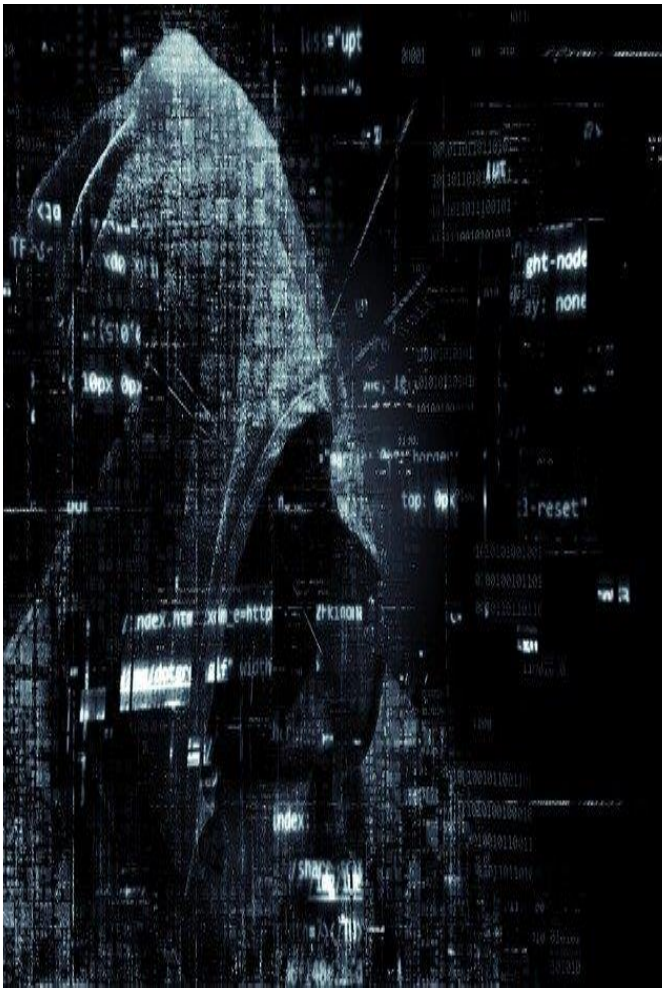
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740723. This communication reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.



# APPROACH

## DESIGNING THE SELF-HEALING SYSTEM ARCHITECTURE

The Self-Healing component consists of three main sub-components (Self-Healing Policies, Decision Engine, Security Rules composer) and three auxiliary sub-components (Parser, Rule Applicator, Logger). Furthermore, they interact with a mapping of the target organisation systems (System Dependency Graph), to extract the information they need for producing automated reactions to protect the target system. As a result of the aforementioned automated actions, the required human interaction, the system maintenance cost and the workload of human administrators is reduced.



# SOLUTION

## SUPERVISED SELF-HEALING

The Self-Healing mechanism is specifically designed to facilitate rapid response to emerging threats, based on the information that the organisation receives in the context of cyber threat information sharing. The aim is to provide administrators with the means to (semi-)automatically and remotely adjust their security appliances to confront cybersecurity threats. As such, it relaxes the needs for many human resources devoted to constant monitoring and adjustment of their configurations. This is particularly important for organisations, such as local public administrations, that have multiple devices to monitor but not necessarily have the required resources. In the context of the CS-AWARE project, an innovative Self-Healing approach has been developed to provide a (semi-automated external Self-Healing system which utilises Cyber Threat Intelligence.

# THE CHALLENGES

### CONTENT DATA AND SECURITY ISSUES

One of the main challenges was the information contained in the data to be input to Self-Healing in order to compose proper machine-readable mitigation rules. Another crucial challenge was the exploitation of cyber threat intelligence data, so as to generate more effective self-healing reactions or mitigation recommendations. Last but not least, the integration with the Data Analysis and the Visualisation components was quite challenging, due to the fact that there was information that needed to be passed from one module to another, while preserving it structured form and the accompanying contextual information.

# RESULTS AND FUTURE WORK

The extensive exposure of organisations to existing and emerging cyberthreats has forced them to invest on mechanisms that efficiently consume shared threat intelligence information and reduce response times in adapting their security posture Self-Healing mechanisms provide the means for administrators to address the complexity of systems management and mitigate potential system faults The proposed solution provides a method to appropriately mitigate cyber threats, while still allowing the system administrator to have control over these actions. 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 commercialisation initiatives of the CS-AWARE project. This will involve a future increase in both the automation and the sophistication of Self-Healing mitigation actions.