7SHIELD

KR04 – Cyber and Physical Threat Intelligence

Scope

Nowadays, with the spread of social networks, blogs and forums, the analysis of these platforms can be an additional source of valuable information on topics such as vulnerabilities that could be used by threat actors or identify anomalous cyber activities, such as knowledge of new malwares and exploits.

Moreover, the Ground Segments are becoming new targets of **cyber, physical and even complex hybrid attacks** and, in this context, the CPTI module is in charge to **prevent** possible attacks, **rising alerts to the Critical Infrastructures** (CIs).

In the frame of 7SHIELD, CPTI outputs are used by SPGU module to improve the Situational Picture overview and to the ENGAGE platform to show identified threats to the CI operators.

Partners

ENGINEERING
Italy

Engineering Group (ENG) is a global player in the digital transformation sector, with relevant expertise in business integration and research and development units focused on different domains such as homeland security, Critical Infrastructure protection against cyber and physical attacks, agriculture, etc.

Contribution

ENG designed and developed the mechanism and the **deep learning algorithms** to retrieve and analyse texts based on specific keywords requested by the Critical Infrastructure operators, searching on **social networks, forums, blogs on the surface, deep and dark web to identify possible threats** that could menace Critical Infrastructures.

Prevention

IoT

All the modules developed in the frame of 7SHIELD have been designed with the consultancy of identified external stakeholders, first responders and following the **requirements** provided by the partners working in the space sector acting as Pilots, who provided the Critical Infrastructures for **testing and demonstration**.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883284

Purpose

The 7SHIELD project is proposing a **Cyber Physical threat Intelligence (CPTI)** module in order to retrieve information from social networks, forums, blogs on the surface, deep and dark web to identify possible **threats** coming from Open Source INTelligence (OSINT) data.

Technology

The CPTI module is based on **recent deep learning state-of-the-art techniques**. These techniques are mostly related to **natural language processing** and **analysis of text sources**.

The main programming language used in the module is **Python** with **microservice architecture** that can help the **scalability** of the module proportionally to the data that should be analysed (i.e. number of text messages).

The CPTI module uses a **MongoDB database** to store requests from the users and CPTI alerts sent to the CI interface.

Contact

- marco.sanbiagio@eng.it

Stakeholders

This solution provides support to the users in order to prepare on time the command center in managing different threats.

It can be used by both the public and private sector, namely:

- the **space sector**
- **satellite ground segment agencies**
- **defense and security government agencies**
- **mobile network companies**

Future Improvements

One of the main issues during the development of the tool was the **lack of data** available to train the AI algorithms. For this reason, we spent the first part of our task looking for open-source annotated datasets of threats and we found one dataset of **annotated threats** on Twitter posts, focusing on the identification of possible threats coming from Twitter posts.

However, the tool has been developed to identify threats in different text data (not only coming from Twitter). For this reason, an improvement of the tool could be the collection of a set of **new data to train the algorithms** and the possibility to add some new threats to be recognized.

www.7shield.eu