OBJECTIVES

PROTECTIVE is a H2020 funded Innovation Action to evolve security alert flow processing into effective solutions integrated into existing security toolsets for Computer Security Incident Response Teams (CSIRTs).

It makes two key contributions to enhance Cyber Situational Awareness (CSA) through:

1. Improved security monitoring and enhanced sharing of threat intelligence between organisations within a community.

2. Ranking critical alerts based on the potential damage that the attack can inflict on the threatened assets and hence to the organisations business.

It provides:

- Correlation engines for alert analysis;
- Automatic prioritisation of security alerts;
- Improved threat intelligence sharing;
- Advanced analytics and visualisation for massive numbers of alerts;
- Constituency context awareness.

AIT · SYNYO · PSNC · theemaillaundry · TECHNISCHE UNIVERSITÄT DARMSTADT · N.R.E.N.R.O. · gmv INNOVATING SOLUTIONS · cesnet · iTTi · UNIVERSITY OF OXFORD

www.protective-h2020.eu

@ProtectiveH2020

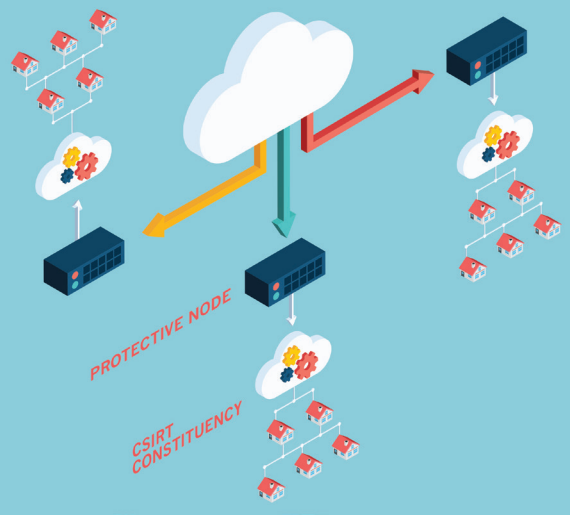
PROTECTIVE

PROACTIVE RISK MANAGEMENT

Enhancing the effectiveness of security alert processing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N0 700071

PROTECTIVE ECOSYSTEM



The **PROTECTIVE ecosystem** provides a number of features to enable fast and **effective security alert processing.**

Security Alert Visualisation provides an immediate overview of the current security situation and allows the operator to drill down for a close in look. She can observe alert trends using a number of time-series algorithms and can project possible attack steps using advanced machine-learning assisted tools.

Security Alert Correlation and Prioritisation reduces the number of alerts to be processed by combining several related alerts into a single Meta-alert which is then annotated with CSIRT constituency information to improve the alert context. The data quality of the meta-alert data is next assessed and finally the meta-alert is passed to the Prioritisation function for ranking against other meta-alerts and presentation to the operator in order of risk importance.

TI SHARING

Threat intelligence sharing is a key feature of the **PROTECTIVE** platform.

The platform ingests security alerts from a wide variety of sources such as firewalls, IDS, honeynets etc. These alerts are converted into a normalised form based on the Intrusion Detection Extensible Alert (IDEA) format. Alerts are then exchanged between collaborating partners through either a peer to peer or centralised sharing architecture.

Each partner decides which alerts it wants to share and these are distributed to all other partners. Automated, rule based, processing is applied to outgoing alerts in order to ensure compliance with information sharing policies and, if required, to anonymise alerts. Meta-alerts may also be shared.

PROJECT USE CASE EVALUATION:

PROTECTIVE will conduct two evaluation pilots during the course of the project based on the following two use-cases:

National Research and Education Networks (NREN) Use case: This validation use-case focuses on real-time sharing of IDEA security alerts between a number of NREN CSIRTS in order to demonstrate the feasibility and effectiveness of the project value proposition. Security alerts from each NREN are forwarded via the PROTECTIVE TI sharing platform to other participants. The scenario is conducted over both pilots. The first pilot will be a limited scope trial with just the three NREN consortium members from Poland, Romania and the Czech republic. Full scope sharing will be evaluated in the second pilot which will involve also a number of non-consortium NREN and other CSIRTS.

SME Use Case: This scenario will demonstrate sharing of large scale threat intelligence with SME's. The trial will be conducted via the project SME partners who are security solution providers. The threat intelligence will be combined with end-use SME computer inventory information to provide targeted, context specific threat advisories. The trial will also evaluate the effectiveness of vulnerability patch management for SME's. The SME use case will take place in the second pilot.