PROTECTIVE
PROACTIVE RISK MANAGEMENT

Pilot deployment

of the first prototype of the PROTECTIVE system at 3 NRENs

Václav Bartoš, Andrea Kropáčová, CESNET

General project information

The PROTECTIVE project aims to provide security teams (CERT, CSIRT) with a toolset enabling greater cyber defence capability through improved cyber situational awareness (CSA).

- Main goal - build a system aimed to increase threat awareness through improved security monitoring, sharing of threat intelligence, ale automatic alert prioritization.
- Establishment of threat intelligence sharing community
- System based on existing technologies (Warden, Mentat, ...)
- To be used by NREN CSIRTs and by SMEs via managed security service providers (MSSP)
- Diverse project consortium: NRENs, universities, SMEs
- H2020 project, 2016-2019

Main system features:

- Advanced alert aggregation and correlation
- Sharing of low-level alerts (from IDS, honeypots, etc.) as well as correlated meta-alerts
- Asset criticality modelling, vulnerability management
- Trust modelling
- Alert prioritization based on criticality of threatened assets and potential damage

Pilot deployment and alert srahing

In the beginning of 2018, the first phase of pilot deployment and testing of the PROTECTIVE system was run. It was focused mostly on collection and basic processing of security alert data and on data sharing among NRENs.

During the pilot, the PROTECTIVE node was installed at three NRENs (CESNET, PSNC, RoEduNet). All of them connected several detection systems, like IDS and honeypots, to the PROTECTIVE node. All nodes were then interconnected and share alert data with each other. Operators at each NREN successfully used the data from their as well as from other detectors to reveal various threats against their networks, as well as to detect infected machines in their own networks.

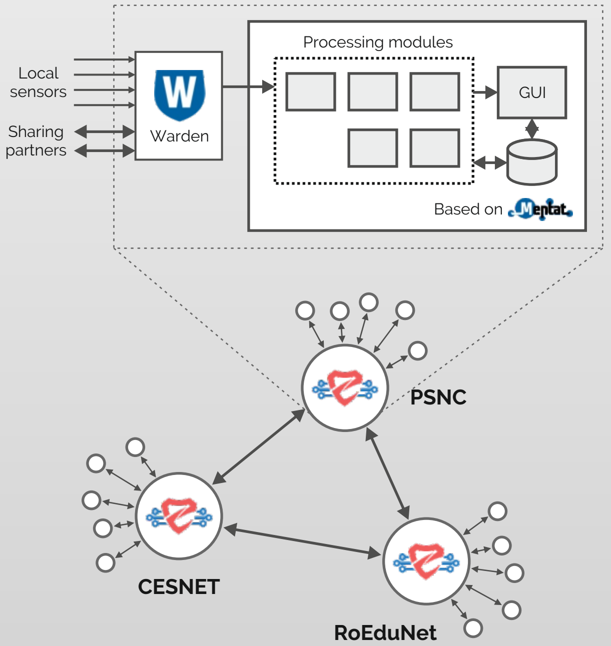
Features implemented and successfully tested in the first phase of Pilot:

- Alert collection and normalization
- Simple enrichment
- Storage, searching, visualization
- Alert sharing

Features tested in the second phase of pilot (currently under way):

- Alert correlation
- Alert prioritization
- Context awareness and mission impact model
- More advanced visualization

PROTECTIVE node
(in the first phase of Pilot)



Local sensors

Sharing partners

Warden

Processing modules

GUI

Based on Mentat

PSNC

CESNET

RoEduNet

The three NRENs are currently sharing alerts from their detection systems in peer-to-peer mode. A mode with a centralized broker will also be implemented to allow larger sharing communities.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement no 700071.

https://protective-h2020.eu/

@ProtectiveH2020

Consortium members: