SCADVANCEXP

NEXT GENERATION IDS FOR ELECTRICITY

Scadvance XP® allows to detect anomalies and cyber-threats in real time in industrial automation networks. It informs about an unauthorized event, indicating the place where the threat occurred, the target of the attack and its probable cause.

STRENGTHS

- FULLY PASSIVE
- SCALABILITY
- SHORT IMPLEMENTATION TIME
- BEHAVIORAL METHODS
- PROBE RESISTANCE TO EXTERNAL FACTORS
- INTEGRATION WITH EXTERNAL SYSTEMS
- VENDOR-AGNOSTIC*

WHY Scadvance XP®?

OT/SCADA systems were designed long before the development of wireless Internet or remote access to systems and networks. The dynamic development of technology did not include OT network security in its scope.

Solution provides with:

KNOWLADGE

Scadvance XP® supports with managing business and operational risk

REAL-TIME MONITORING

Scadvance XP® defends processes production

PROCEEDING THE INCIDENT

Scadvance XP® adapts procedures to legal requirements

OT/ICS NETWORK VISIBILITY

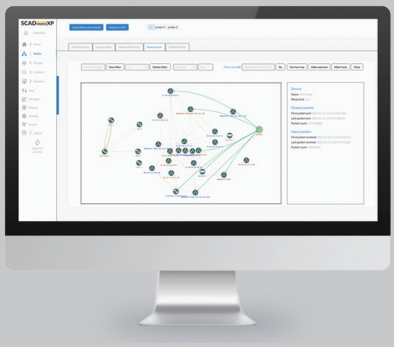
Scadvance XP® monitors industrial networks not on their edges as standard IT systems do, but collects CAN information directly from inside them, analyzing all transmitted packet traffic.

The applied hardware interfaces allow for monitoring and connection to all industrial automation networks, thus the persons responsible for security in the organization have visualization of all existing connections and devices in real time. As a result, they can see unwanted communication in the OT network.

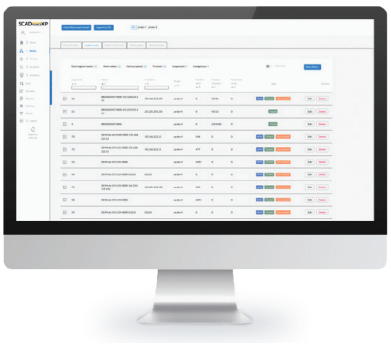
- real-time network audit
- ability to record traffic
- immediate visibility of the network map, information about connected devices
- external vendor traffic tracking

PASSIVE AND AUTOMATIC ASSET INVENTORY

The **Scadvance XP®** system detects devices connected to the protected network on the basis of observed traffic. In this way, a map of the protected network is created in the form of a graph of connections between network devices at the level of network logic devices.



- detection of devices connected to the protected network based on passive observation of traffic
- analysis of traffic between devices (type and number of protocols, packets, ports and many others)



DETECTION OF CHANGES IN THE NETWORK

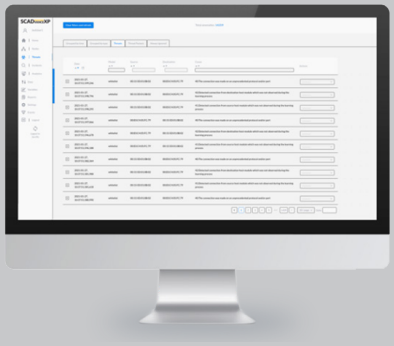
Scadvance XP®, by analyzing the correlation of anomalies and results of the work modules AI detects the most dangerous and unobserved anywhere else attacks.

The system has mechanisms that allow to build prediction models dedicated individually for each logical connection separately, which significantly improves the quality of prediction and anomaly detection.

- automatic detection of anomalies, attacks and breakdowns
- automatic building of dedicated predictive and analytical models

REPORTING

Scadvance XP® allows you to create and customize user views and reports according to permissions and preferences.



- presentation of traffic statistics in a protected OT network using built-in and configurable dashboard
- reports presenting the state of the network (status, scoring)
- device inventory reports
- reports supporting network hardening (subnets, protocols, devices)

ICsec S.A. is a leader on the industrial infrastructure security market, in particular for enterprises with industrial infrastructure. ICsec designed and built the Scadvance XP® system (IDS class intrusion detection system), intended for monitoring the OT network. The solution addresses the needs related to the monitoring of industrial automation networks, detection of potential threats and anomalies in the traffic between devices connected to the network.

ICsec S.A. | ul. Wichrowa 1A, 60-449 Poznań, Poland | GSM +48 506 931 953
biuro@icsec.pl | www.icsec.pl