SIEMENS

Ingenuity for life

Industrial Anomaly Detection

Reliable detection of threats in industrial networks

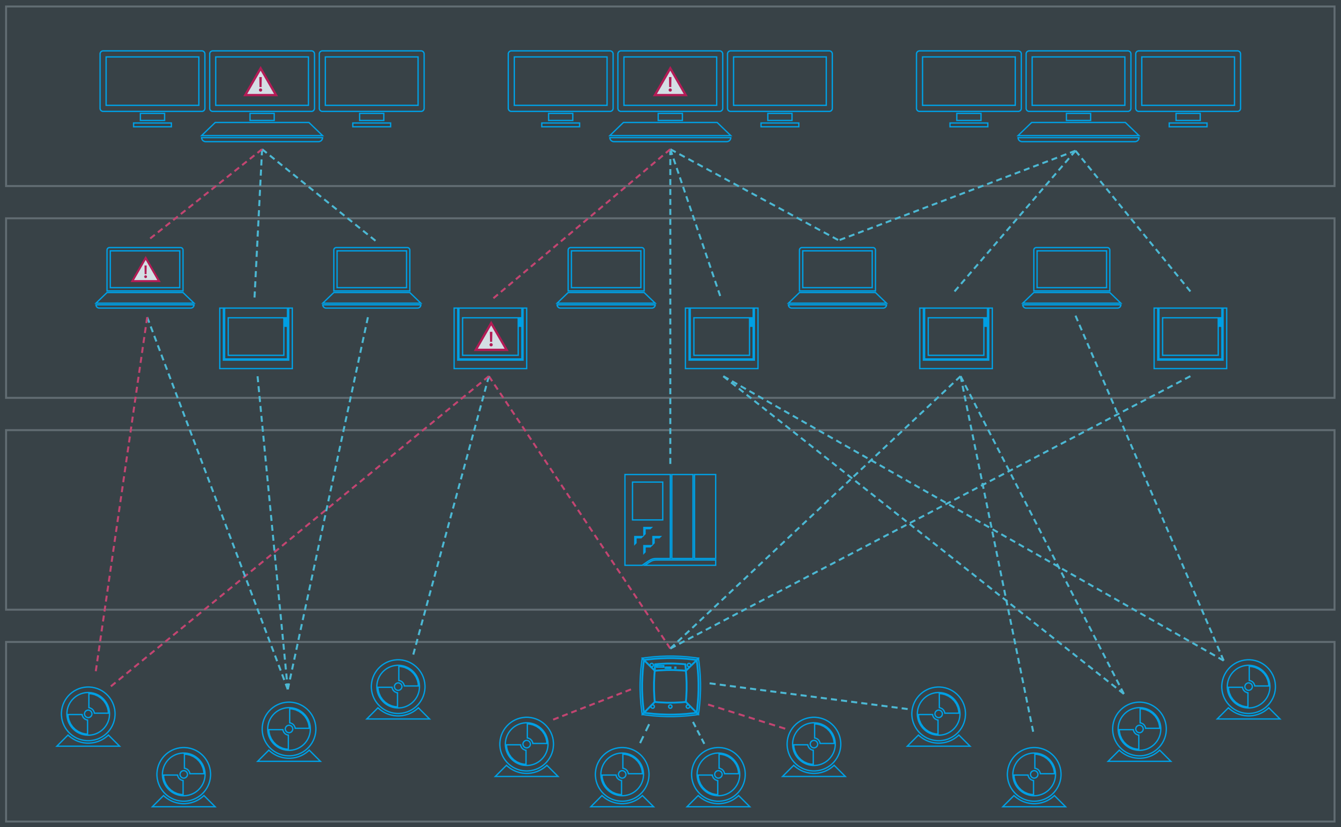
As digitalization advances, plants and machinery are becoming increasingly interconnected. And yet these complex industrial networks are far less protected against cyber attacks than office IT. In most cases, protection is handled by firewalls, endpoint protection in some equipment, and deep packet inspection at the gateway to production and office networks. There is no transparency over the normal communication of controllers or operating units. Detecting malware in the production plant network as well as in new or modified assets is not possible.

Solution architecture for identifying anomalies

The solution to this problem is industrial anomaly detection, which can be seamlessly integrated in industrial networks. It is easy to implement and provides full transparency over the connected systems. As a result, you not only know which assets belong to the network but also how they communicate with each other. Deviations can therefore be easily detected and investigated by the local personnel. Industrial anomaly detection supports many different manufacturers and protocols and relies on machine learning to keep the configuration simple.

Benefits

- Greater transparency over the assets in industrial plants
- Early, self-learning detection of cyber-threats
- Passive data collection with no impact on production
- Important addition to the comprehensive defense-in-depth concept



Industrial anomaly detection not only shows which assets are present in the industrial network, but also the communication flows among the devices and with the IT network.

Switches connect the systems in the plant network topology, which is usually ring- or star-shaped. These switches often also make it possible to mirror the entire data traffic via a so-called SPAN port, where the anomaly sensors pick up the data and enable evaluation. The software is preinstalled on an industrial PC (IPC) from Siemens. It can also be easily installed on the Ruggedcom RX1500 platform and is thus easy to integrate into industrial environments.

Industrial anomaly detection also uses Machine learning, which enables a self-learning system configuration. The software automatically analyzes the data traffic on the network during a learning phase so that it can detect anomalies later on.

These may indicate, for example, hacker penetration or data theft. Since anomalies can resemble changes to equipment configuration or software updates, the system alerts the technical staff each time a deviation is detected so that they can quickly review the situation. Anomaly detection is particularly suitable for companies in the automotive industry, aerospace, pharmaceuticals, the chemical industry, as well as the food and beverage industry.

Siemens AG
Digital Factory
P.O. Box 48 48
90026 Nuremberg
Germany

Article No.: DFCS-B10159-00-7600
Printed in Germany | fb 8029

siemens.com/iss