CyberLympha®

Establishing OT Security

CyberLympha approach

The purpose and scope of this document

This document contains a brief analysis of the contemporary situation in the field of operational technology and industrial control system security. An approach to establishing and maintaning asset security is outlined and compared against existing strategies. This comparison is based on the findings of the actual product testing that has been performed in CyberLympha product testing labs.

The purpose of the document is providing the reader with relevant information on overall approach, functions and features of the compared solutions.

The target audience of this document is the engineering staff and managers, responsible for maintaining OT security for their companies as well as current and perspective Partners.

Securing industrial assets: the problem

Contemporary industrial control systems (ICS) are connected to all sorts of internal systems that operate on Customer's infrastructure as well as to a number of external systems accessible via the Internet making operational technology (OT) segments truly complex. However, while ICS architecture has evolved, and convergence between IT and OT segments is bringing the era of "air-gapped" systems to its end, the basic control processes remain the same. Often enough within the increasingly complex OT infrastructure legacy industrial control systems are still in operation.

The rapid development of emerging digital, information and telecommunication technologies, including the development of technologies encompassing *Internet of Things*, *Industrial Internet of Things*, *eXtended Internet of Things* and *Industry 4.0* in recent years has led to a significant change in the IT landscape, and consequently in the specter of threats to information security of the OT environments. Modern OT comprises a mix of complex cyber-physical systems integrated both with each other and with higher-level systems such as ERP of plant management software systems, widely using the Internet and cloud as well as wireless communication technologies.

The set of factors affecting the security of the OT has therefore changed – in addition to the traditional factors, new ones have emerged, caused by the ongoing changes in the information and telecommunications landscape of the IT and OT, which entail a change in the qualitative nature of threats and vulnerabilities: an expansion of the attack surface and applied attack vectors range as well as a general increase in the number of cyberattacks and the criticality of incidents related to OT security.

At the same time, OT retained unique and specific characteristics that make traditional security systems less efficient while operating with OT assets.

Contemporary factors influencing the safety of an OT infrastructure include the following:

- High level of criticality of the consequences of safety incidents or incorrect intervention in the operation of the ICS, which can lead to equipment failures or changes in operating modes and, as a result, major industrial accidents, death or damage to human health, environmental disasters. On the one hand, this makes OT an attractive target for attacks, on the other hand, it makes it difficult to choose and deploy response actions to counter the attacks
- Use of industrial communication protocols for internal information exchange and interaction between the assets, incl. proprietary vendor-specific protocols, use of IoT technologies, which often enough carry multiple unknown or undiscovered vulnerabilities. At the same time many traditional IT components, such as Windows / Linux operating systems and network equipment, that are characterized by both well-known and described as well as yet undiscovered vulnerabilities are widely used within the OT infrastructure

- Lack or significant shortcoming of deployed protection mechanisms, such as: user and node identification and authentication, network segmentation and protection of OT assets from DoSand DDoS attacks, protection of data transmission and control commands, configuration and code integrity control, control over process and applications start/stop, user privilege differentiation, and finally event logging. This factor contributes to the weakness of the system resistance to OT-related cyberattacks greatly
- OT security is also heavily influenced by the fact that the many ICS have been in operation for many years, often decades, possess outdated component design that may have severe security flaws. Updating and upgrading the OT infrastructure is often a mind-bogglingly difficult task due to process criticality and equipment incompatibilities, especially between legacy and newer systems. These factors often complicate or make gradual upgrades impossible, consequently leading to updates being cyclically postponed to a later time or not carried out at all
- A growing level of integration of the modern OT systems with various IT systems makes OT environment no longer isolated, but rather an important part of the enterprise infrastructure. A wide adoption of wireless communication technologies as well as cloud and IoT cloud integrations expose OT for attacks coming from both outside and inside of the corporate network
- The evolution of adversary techniques and tactics has decreased the time required by the malicious party to access, recon and deliver the impact to the industrial networks and assets. While ICS remains a harder target for many, the number and skills of those who operate on the other side of the security battle have established themselves as important concerns. Defending against skilled and persistent adversaries leaves security teams in need of means of discovering, confirming and mitigating the attack in the most speedy and precise fashion
- Lack of skilled personnel responsible for maintaining secure OT operation, especially considering the fact that the personnel often has privileged access rights to the assets, as well as the fact that asset maintenance is often performed by external contractors. Due to the openness of the systems, maintenance can be carried out remotely, incl. connections from unprotected workstations. When working with OT assets, personnel tends to focus on operations management, thus failing to provide the necessary attention to the issues and concerns of information security

We can easily deduce that modern OT includes highly critical systems, and yet is open and vulnerable to cyberattacks, either directly from the Internet, incl. cloud IoT environments and/or from corporate (IT) networks, or even over internal wireless channels. Most OT infrastructures have no efficient built-in mechanisms focused on establishing security, monitoring and enforcing configuration and vulnerability control. The ineffectiveness of the traditional IT tools in protecting the OT makes cyberattack detection and response a difficult task.

To further prove the point, experts agree that OT environments and ICS in particular require a special approach that accounts for their unique properties and features.

CyberLympha approach to establishing OT security

To ensure that Customer's security operations team gets the most accurate and relevant information we analyze, process and correlate the data collected from several input sources. Different attack vectors have different signatures and require different response & remediation tactics. Here are the four important cornerstones of establishing and maintaining security in the industrial environment:

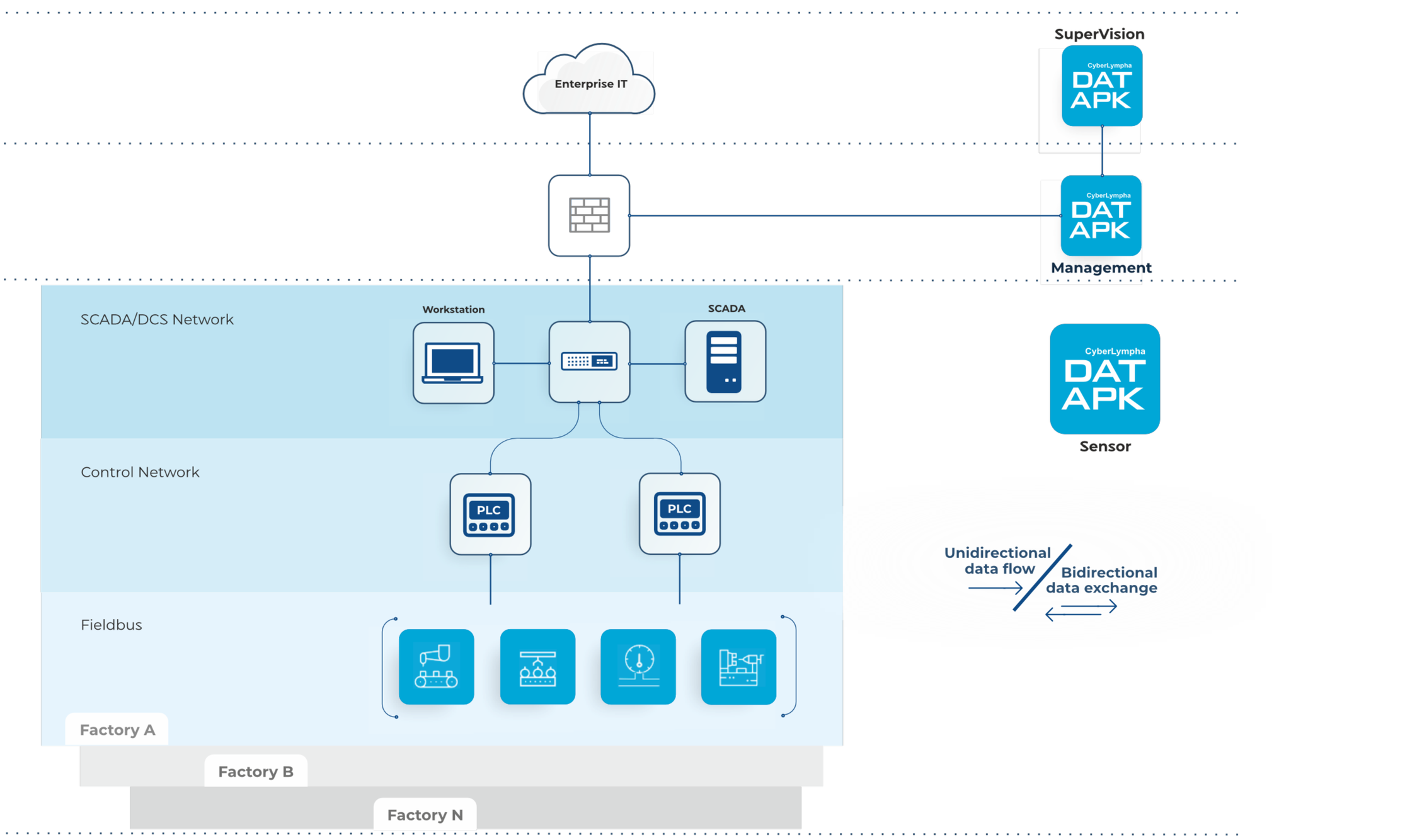
- Many hacker attacks begin with unauthorized network access. Monitoring all **OT network** traffic enables us to detect malicious nodes and traffic as soon as it appears on the network
- Insiders that try to initiate the attack using existing legitimate nodes, for example plugging in a USB stick, change asset configuration. We keep a **catalogue of reference configurations** for instant change detection and remediation

- Events generated by the assets are an invaluable source of data concerning system operation. **Event collection and enrichment**, essential for precise incident detection, powers quick and on-target response
- Hackers attempt to use exploits whenever possible. We **scan the assets for possible vulnerabilities** and provide security personnel with lists of detected caveats that require updates or configuration changes
- Our key focus is providing a comprehensive OT security monitoring solution including anomaly detection to businesses of any size from any industry, including Customers that operate critical infrastructure
- Often enough industrial infrastructures include multiple sites that may have a significant geographical span. Our solutions fit any infrastructure, be that a relatively small single-site power plant, multiple production sites dispersed throughout the region or a vast network of hundreds of small sites connected by low-bandwidth WAN links – we know how to address each task and provide every security measure without compromising asset operation

This approach enables us to protect different OT infrastructures operated by the Customers from various industries:

- Oil and Gas
- Energy and Generation
- Chemical industry
- Nuclear energy
- Metallurgy
- Water processing plants
- Automotive and other manufacturing facilities
- Other industries

A typical diagram of a CyberLympha OT security system is provied below.



Comparing approaches

CL DATAPK covers all important cornerstones of ensuring the protection of the OT environment and ICS. Additional features of the CL DATAPK make it flexible and easy to integrate and operate, which in turn allows Customers to build a DATAPK-based OT Security system of any complexity and scale, protecting their assets against existing and emerging threats.

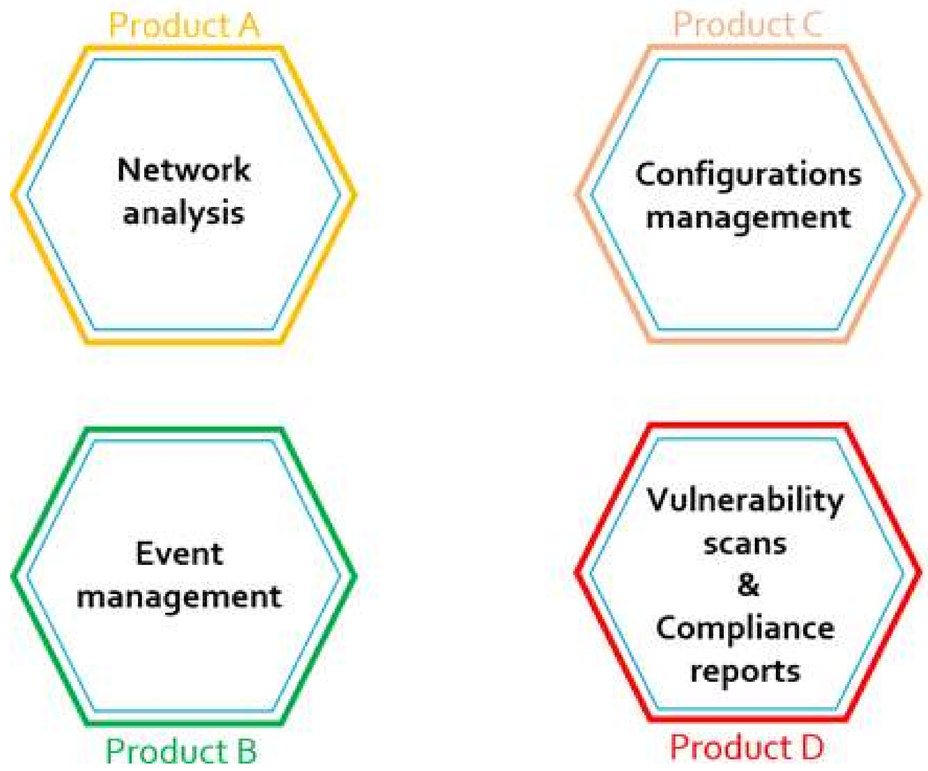
Most competitive solutions focus on passive traffic analysis technologies, as this approach is an immediate and the easiest answer to a typical Customer fear that implementing security measures in the OT infrastructure may lead to disruptions in system operation and thus will cause an outage.

However, the data, collected via the active security solution component that utilizes legit ICS commands and protocols built into the OT assets holds a significant additional value and allows for a qualitative improvement in the detection and asset inventory capabilities of the solution.

Due to this reason solutions that exclusively rely on passive network traffic analysis can be expected to be left behind in midterm future. Most of the companies competing on the market are aware of this and have their active components in development or already existing as stealth products that would be brought out when the vendors feel that the asset owners are ready[1].

Building a comprehensive OT security solution that incorporates a passive-only OT security product is a task that includes integrating several different products with all limitations and difficulties that arise from using heterogeneous or multi-vendor solutions:

- **Product A.** Network analysis
- **Product B.** Event management
- **Product C.** Configurations management
- **Product D.** Vulnerabilities and compliance management



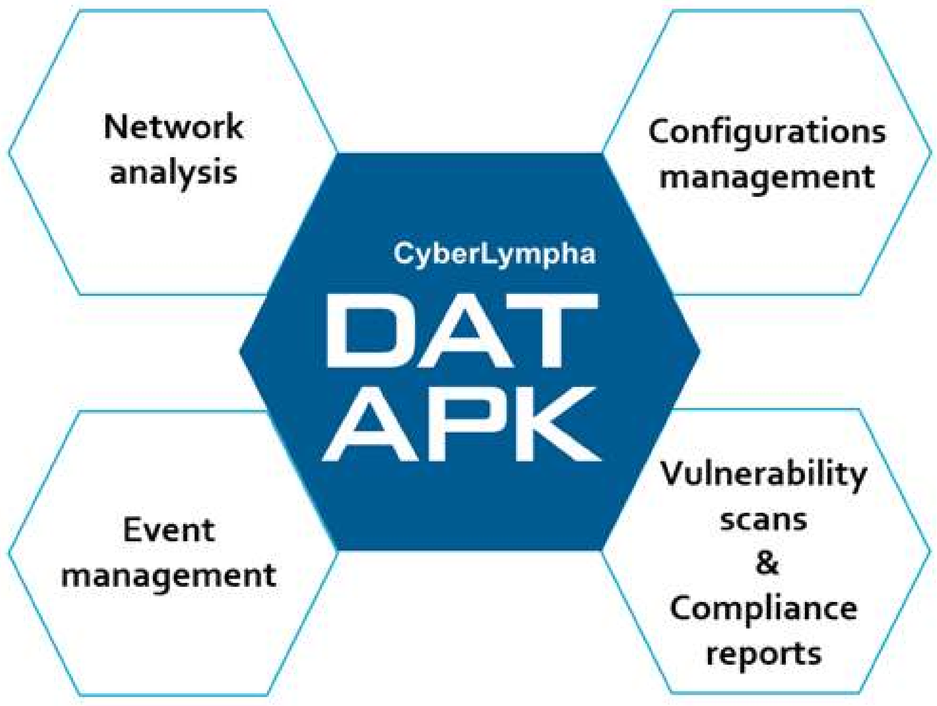
The significant advantage of the CyberLympha approach over the competition is that it unifies functionality of several security product classes in one solution. In addition to extensive traffic analysis capabilities CL DATAPK performs:

- Network and node configurations collection and control
- Inventory information and event logs collection from assets' OS

The benefits for the Customer are lower TCO and OpEx as well as horizontal and vertical solution scalability. CyberLympha products cover every requirement for OT security.

---

[1] According to Dale Peterson, The Future of the ICS Cyber Security Detection Market



For example, CyberLympha's flagship product, CL DATAPK, supports both query (active) and observation (passive) operation modes, allowing the Customers to strike a balance between security efficiency and impact risks.

Agentless operation is another important advantage of CL DATAPK. All data is collected using mechanisms and protocols built into the assets. This is especially relevant for highly critical OT infrastructure.

CL DATAPK is based on a modular architecture that allows flexible adaptation to Customer's OT infrastructure of any scale and complexity. Adding vulnerability descriptions and event correlation rules in response to changes in threat landscape or expanding supported protocols lists can be performed on the fly without the need to modify product code or wait for patches and updates. This allows CL DATAPK to support security deployments for both new and legacy systems designed by different vendors that have established presence in for various industries.

Conclusion

The main difference of the CL DATAPK from the competition is the ability to operate in active mode, that utilizes protocols and mechanisms built into the assets to collect additional data without impacting asset operation, in addition to traditional passive mode that solely relies on network traffic analysis.

Based on the product features comparison CL DATAPK has better overall solution capabilities:

- Comprehensive security monitoring, including network analysis, asset inventory, event processing and vulnerability scanning
- Sophisticated asset inventory that includes hardware, software and process configuration management functions for all types of assets
- Ability to monitor and detect attacks that start with asset configuration changes (i.e. using USB sticks).
- Ability to correlate data collected from different sources, such as network traffic and asset events
- Scalability ranging from all-in-one single box deployment to multisite hierarchical installations
- Ability to adjust to any protected asset type, including both legacy and newest systems as well as highly customized OT environments

These capabilities allow our Customers to lower both TCO and OpEx, requiring less staff and allowing the security operations to automate routine security check-up tasks.

In order to facilitate and prove the conclusions given in this document we strongly recommend solution testing on Customer infrastructure.