Industrial system cybersecurity:

questions of feasibility and the defense-in-depth strategy

kaspersky bring on the future

Contents

Introduction

The particularities of providing information security to industrial systems largely stem from the fact that information is not their primary focus. In office IT systems, the main asset is data stored on devices or transmitted over networks, but the industrial networks essentially serve to support the operation of physical production equipment and infrastructure. Evidence of this can be found in safety regulations across **various industries**[1] , which indicate the primary values for operators of industrial systems: the physical safety of equipment and personnel, the continuity of production processes, and system performance. Data is not included in this list.

Because of that, industrial system owners are reluctant to invest significant resources in solutions that ensure information security.

When a buying decision is made, these companies expect that a security solution would not only detect and block cyberthreats but also help address pressing engineering challenges more obviously related to core activities, such as detecting configuration errors in controllers. This extended functionality might be an additional motivating factor in making a purchase or even be perceived as the sole value, leading to the choice of a solution that is less useful from a cybersecurity perspective. In general, when considering information security issues, companies often lack a strategic approach.

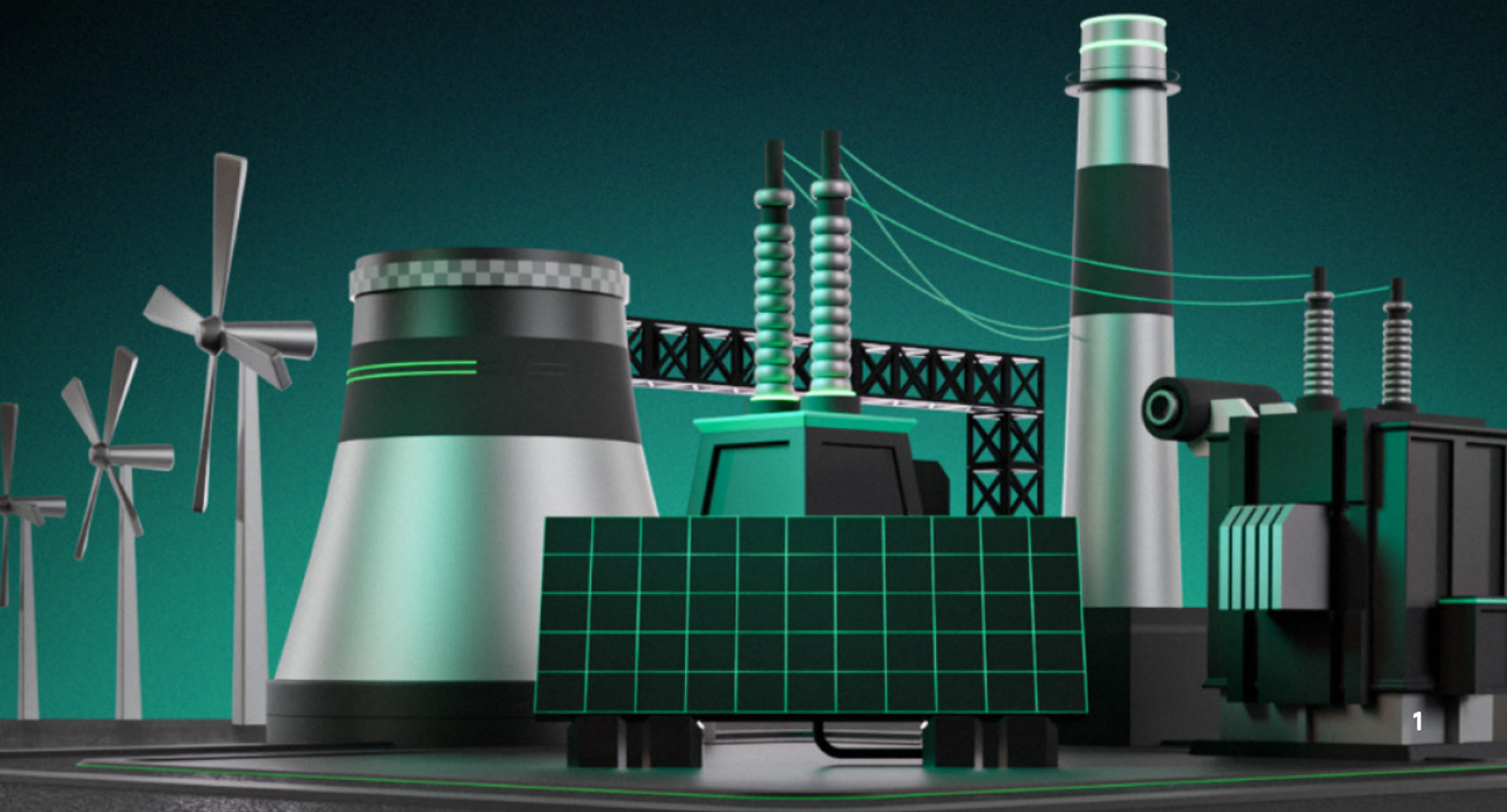
In this article, we will discuss both the feasibility of protecting industrial information systems and the approach to it using the example of the defense-in-depth strategy, which, based on our experience, is a good fit for industrial environments.

[1] For example:

Regulatory norm "Criterios generales de seguridad para la operación de reactores nucleares de potencia" (Directorio de la Autoridad Regulatoria Nuclear, Argentina)

Regulatory norm "NR11 - Transporte, Movimentação, Armazenagem e Manuseio de Materiais" (Comissão Tripartite Paritária Permanente (CTPP), Brazil)

Guidelines manual "Manual de Normas de Bioseguridad y Riesgos Asociados" (FONDECYT – CONICYT, Chile)



Feasibility issues

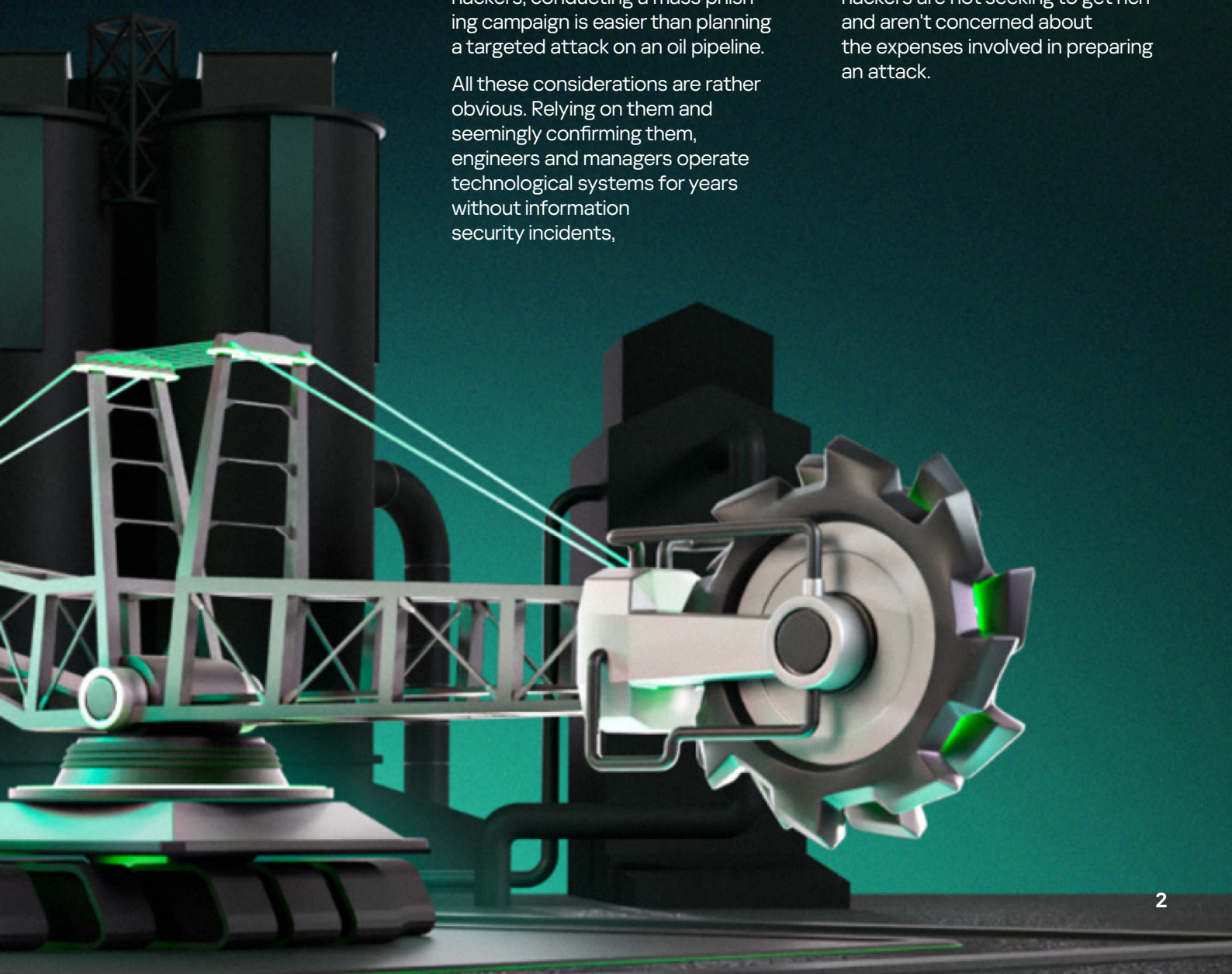
The question "Is it necessary to enhance the protection of an industrial system?" boils down to two aspects: practical and economic feasibility.

Practical feasibility

Compared to office networks, industrial systems are more difficult to attack, making them less attractive to malicious actors. They are often isolated from external networks, and many system owners consider this isolation to be a sufficient security measure. Moreover, technological software, whether it's SCADA systems or PLC configuration files and code, is more specialized than the usual combination of Windows and Microsoft Office and requires criminal groups to conduct additional research to launch attacks. As a result, for profit-hungry hackers, conducting a mass phishing campaign is easier than planning a targeted attack on an oil pipeline.

All these considerations are rather obvious. Relying on them and seemingly confirming them, engineers and managers operate technological systems for years without information security incidents, and they believe that additional security measures will continue to be unnecessary in the future. Of course, this approach overlooks the possibility that the lack of observed incidents might be due to imperfect monitoring tools: an attack could simply be missed, especially if attackers are not in a hurry to reveal themselves.

Additionally, in recent years, we've seen a sharp increase in politically motivated attacks on critically important industrial systems conducted by hacktivists or state-sponsored groups. These hackers are not seeking to get rich and aren't concerned about the expenses involved in preparing an attack.



Economic feasibility

Industrial systems are assets with a long payback period, often 20 years or more, and even longer planned operational periods. Many modern systems which are currently around 10 years old were deployed as a single set of equipment and software.

The possibilities for updating and correcting the installed software are, at best, limited – if provided at all. Upgrading such complexes is comparable in cost to replacing them, and it's not economically viable to perform upgrades before the end of their service life.

The table below shows the choice that the owners of such systems face:

	If a new security solution is implemented	If a new security solution isn't implemented
Definite negative effect	Expenses for procurement, compliance testing, acceptance testing, and deployment	
Definite positive effect		No additional expenses for a new security system
Possible negative effect	Disruption of industrial processes during the implementation or operation of the security solution	Losses in the event of a cybersecurity incident
Possible positive effect	Defense against cyberattacks and protection against associated losses	

Table 1. Feasibility matrix for implementing a security solution

Thus, on one side of the scale for the enterprise are specific and quite significant expenses for acquiring, testing, and deploying protection. To reduce these expenses and make them operational as opposed to capital, an **MSSP**[2] subscription model can be used, with the industrial corporation's information security infrastructure managed from an external monitoring center owned by a service provider.

On the other side of the scale is a cybersecurity incident, with an unknown probability of occurrence and unknown magnitude of possible losses caused. To decide in favor of purchasing protection, either a definite significant positive effect must be assumed, or the risks of a cybersecurity incident must be accurately assessed (and compared to the costs of implementing security software), which is not always possible. While high-profile cases, such as the disruption of the Colonial Pipeline in 2021 or the accident at the Iranian Khuzestan Steel Company in 2022, demonstrate the capabilities of attackers to cause large-scale disruption of industrial processes leading to serious losses, companies need more systematic and comprehensive information about these and similar cases to see if they are relevant to their own situations.

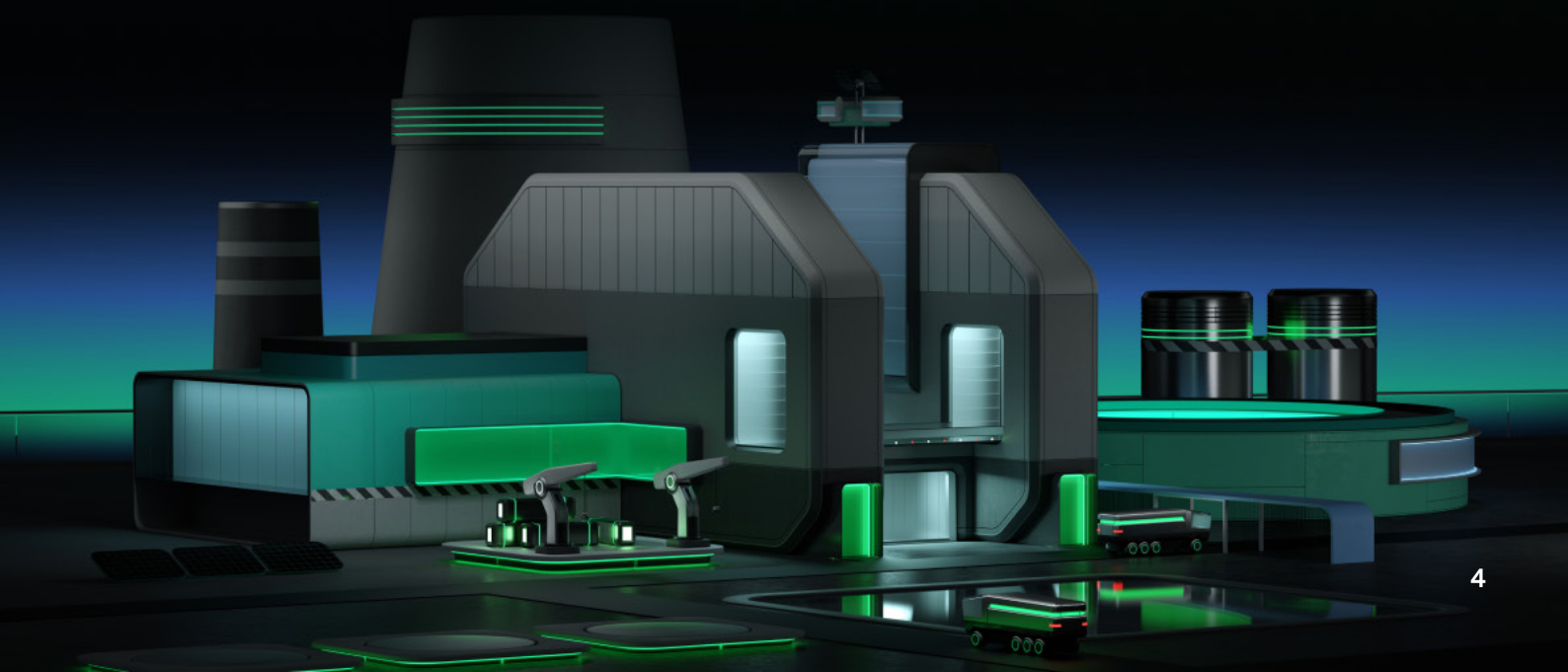
[2] Managed security service provider

Implementation issues

But let's assume that the company management, after assessing the risks, concludes that it's necessary to protect their operational technologies (OT), finds a window of opportunity (for example, the time has come to replace systems or introduce a new system) and a budget for changes. How best to ensure protection?

Industrial security solution providers such as Check Point, Fortinet, Cisco, and Schneider Electric, as well as regulatory bodies in different countries, recommend and support a multi-layered approach called **"defense in depth"**[3]. It creates a set of mutually supportive measures that provide system protection by controlling equipment, data, applications, processes, and personnel. Let's consider the components of its typical implementation.

[3] See, for example, the report "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" by USA Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center and Industrial Control Systems Cyber Emergency Response Team.



Hardening the system by reducing the attack surface

The process of system hardening involves carrying out an inventory of all used devices, connections, applications and software components, accounts, processes, services, ports, and protocols. After the inventory, these assets are divided into two groups: those not necessary for the enterprise's operation are disconnected, while the rest, if necessary, are reconfigured according to the information security requirements. For example, privileges for accounts must be restricted to the minimum necessary (specifically, disabling remote access unless it's mandatory for the role in question).

Processes should operate in the same way, with the minimal required rights. All operational and system software for which there are updates must be promptly updated.

Generally, convincing system owners of the value of inventorying is easier than for other security measures. Asset accounting is a clear and necessary task, essential for the operation of the enterprise and, in some jurisdictions, even mandated by regulatory requirements. In the context of Table 1, it has a definite positive impact, and security solutions offering this capability are inherently more understandable and useful for enterprises.

During the inventory process, the industrial system owner and the security solution provider, working together and drawing from the specifics of the particular system as well as their industry and technological expertise, identify cybersecurity risks to which the system is exposed. This information is crucial for subsequent protection stages within the defense-in-depth approach.

Inventorying is a substantial and complex process. It cannot be effectively conducted without automation, especially in distributed systems such as power grids. Existing inventory methods include, in addition to manual inspection, analysis of configuration files, passive analysis of ICS network traffic copies, and active polling of ICS devices. Note that the last method is more invasive and may not be suitable for all enterprises. It should be applied with caution. It's also important to understand that inventorying is a process, not a stage: the data about the system's information assets and their relationships and connections must be updated continuously. This process creates a picture of the system's normal behavior, which is subsequently used as a benchmark. Moreover, by comparing the inventory results with project documentation, unnecessary or unaccounted-for assets can be identified.

[4] See, for example, the report "Recommended Practice for Patch Management of Control Systems" by USA DHS National Cyber Security Division Control Systems Security Program.

On a separate note, we should mention here the issue of updates, which cause serious concern among operators of industrial facilities. In reality, for modern systems, the update process can be relatively painless. But of course, certain rules must be followed. Here are the most important ones:

Technology software must be updated systematically, but independently from corporate software updates. It must be done according to industrial process requirements, during equipment maintenance periods[4].

Before deployment in the production environment, updates must be tested in a similar test environment to prevent unforeseen consequences.

It should be possible to update offline or from a local server.

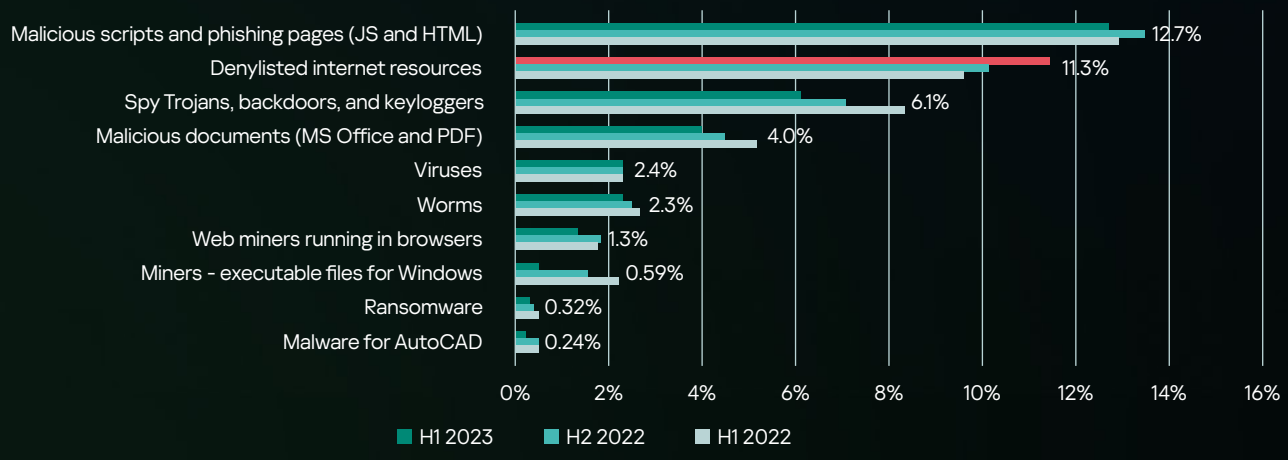
A mechanism for rolling back updates is necessary.

These requirements also apply to updating security software at industrial facilities.

As mentioned earlier, real systems often use outdated software no longer supported by vendors or versions of operating systems for which updates are no longer released (sometimes the system is intentionally not updated to avoid any negative impact on processes). In such cases, the role of the security solution is even more important: it must support this legacy software and protect against exploitation of vulnerabilities that have not been patched due to the lack of updates.

Enabling available protection measures

Concerned about the integrity and continuity of industrial processes, ICS operators are cautious about implementing any protection inside industrial systems. They often believe that securing the network perimeter to prevent threats from entering is sufficient to ensure safety. However, in reality, a significant portion of security incidents occur due to the actions of users within the protected perimeter.



Percentage of ICS computers on which malicious objects from different categories were blocked

Above are statistics on the types of malicious objects whose activity was thwarted in the first half of 2023 on ICS computers connected to Kaspersky Secure Network. It's worth noting that these statistics apply not only to critically important facilities but also to computers in other areas related to the activities of industrial enterprises. Engineering and industrial software is frequently installed on engineers' office laptops, in testing laboratories and research centers, at technical universities, on utilities sector facilities, and elsewhere.

Though Identifying threat sources is not always straightforward, we can confidently say that the incidents at the top of the list above involve users opening phishing pages and prohibited resources on the internet, as well as malicious MS Office and PDF documents. To swiftly detect such actions, protection is needed at the node level (that is, computers and similar devices) based on lists of allowed or prohibited processes and applications. The configuration of ICS employees' devices changes less frequently than in corporate networks, so these measures, with their minimal invasiveness, can be quite effective.

Continuous monitoring of the security of ICS, networks, and connections

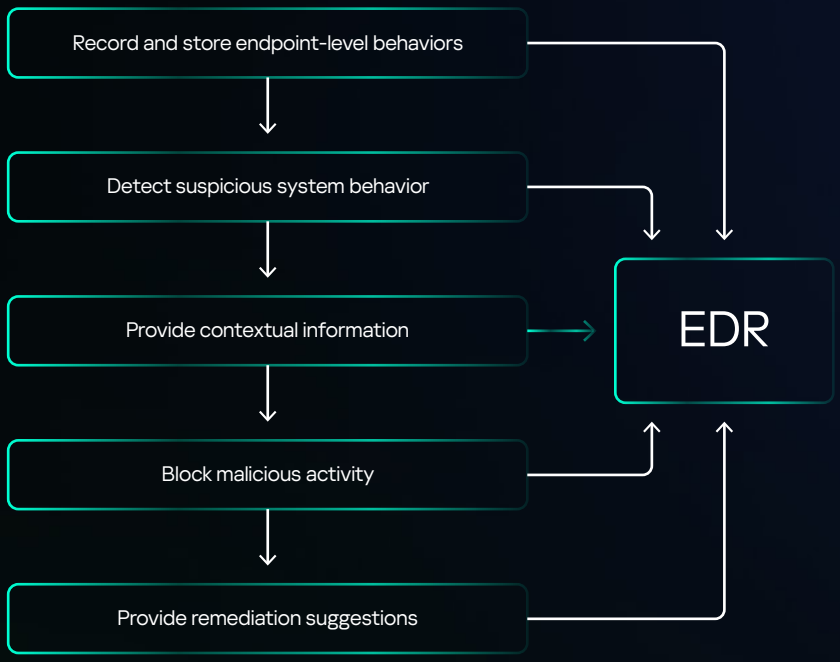
Unfortunately, not every component of an industrial system can be protected as easily as employee devices. For instance, PLCs, which act as intermediaries between physical equipment and SCADA systems, have closed architecture and use real-time operating systems with limited memory. It's not feasible to install security solutions that continuously monitor their operation directly on them. PLCs are supposed to be created following the safe-by-design principles, but we and our colleagues have repeatedly demonstrated that it's possible to decipher the protocols and file formats **used by these devices**[5]. This means that PLCs are almost as vulnerable as regular workstations.

If it's impossible to install protection directly on the PLCs themselves, and yet they must be protected, the security solution must track threats on their way to the device. However, there are nuances here: allowing security solutions to block PLCs (or SCADA systems) when a threat is detected is dangerous. Therefore, monitoring functionality that alerts operators about abnormal behavior or malicious activity is especially important for industrial networks. For PLCs, this could involve integrity configuration checks; for SCADA systems, it might include analyzing mirrored traffic.

What should be monitored specifically? Firstly, it's essential to track network connections to and from remote hosts and check devices connected to USB ports. Secondly, registering other abnormal activities, such as running of unknown processes or changes to key files like SCADA projects, is crucial. To detect anomalies, the picture of the system's normal state obtained during the inventory is used as a benchmark. Finally, the protection must identify malicious files and processes by signatures, although heuristic analysis capabilities are also important when updates are less frequent.

Solutions that record and store endpoint-level behaviors and use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems are classified as EDR (Endpoint Detection and Response).

[5] See, for example, the paper "ICSREF: A Framework for Automated Reverse Engineering of Industrial Control Systems Binaries" presented by Anastasis Keliris and Michail Maniatakos at NDSS 2019.



A significant function of EDR solutions, such as Kaspersky Industrial CyberSecurity for Nodes, is the ability to transmit event information to other systems (such as SIEM, MES, BI) for storage and further analysis. Some incidents can only be correctly identified by comparing information from different nodes – for example, a single login attempt with an incorrect username–password pair might be an operator's mistake, but if it happens repeatedly on different machines, it is likely a sign of an attack. Solutions that can correlate data from various sources fall into the category of XDR (Extended Detection and Response).

Managing ICS and technological network security based on risks

The results of risk assessment obtained during the inventory process are used to establish security policies. Here it's essential to match response measures with threats. For example, upon detecting a cryptocurrency miner on an ICS computer, there is no need to immediately disconnect the host, as the consequences of such disconnection might be more critical than the damage caused by the miner itself. The risk framework and corresponding policies must be promptly updated as new threats emerge.

Human factor management

As mentioned in Section 3.2, many security incidents in OT systems, like in corporate IT systems, stem from user actions. To combat operator errors, enterprises must implement data and information system handling policies for employees. Operator work instructions should also be drawn up taking into account information security requirements. Employees should know how to act in different situations and understand that they are accountable for their actions. Consequently, if an incident has occurred, the system should trace its initiator whenever possible. The measures discussed in Section 3.1, such as limiting user rights to the bare minimum necessary, help to reduce the frequency and severity of such events.

Possible implementation

In this context, Kaspersky occupies a unique position in the market. The company has been operating in the field of cybersecurity for 26 years, with over 12 years dedicated to developing solutions for protecting industrial networks. We collaborate with industrial automation solution vendors to learn from each other's experience and create compatible products. For example, all our security updates are tested in conjunction with software from leading manufacturers. Our strong market position allows us to allocate the necessary resources for research, without worrying about quick returns on investment. For example, we can hire specialists from various industrial sectors and employees of leading automation vendors with practical knowledge of the operation of industrial systems, enabling us to fully understand the customers' needs and concerns.

Currently, the manufacturers of automation equipment, such as ABB Ltd., Schneider Electric, Rockwell Automation, General Electric Company, Honeywell International, Inc., and Siemens AG, are also the market leaders **in industrial system security**[6]. However, the security tools they offer are usually highly specialized and not very effective. This is not surprising: for ICS manufacturers, security development is a secondary focus, so they are not strongly motivated to develop a broad cybersecurity perspective. Moreover, they are not particularly willing to allocate generous budgets for these purposes. For the implementation of a comprehensive approach, such as defense in depth, these solutions are unsuitable.

Meanwhile, there are not many ICS security solutions from independent vendors on the market. One of the main challenges here is gaining access to the actual industrial systems for development and testing. Few companies can afford to build a test metallurgical plant to create and test protection for real plant's OT systems, and it's virtually impossible to try and take into account all the details, processes and possible scenarios without practical testing.

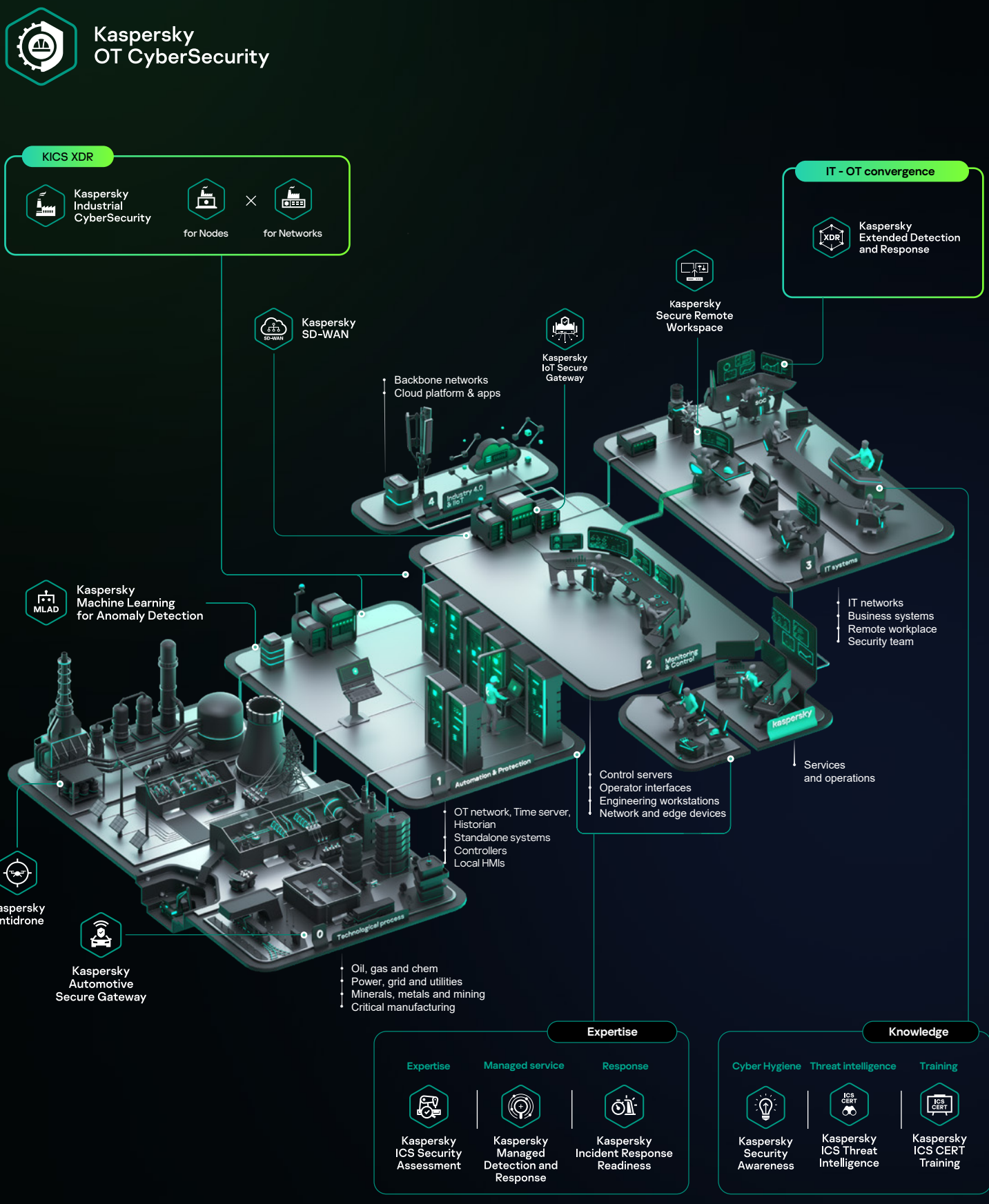
The problem is partly solved by simulating physical components, but this task also requires expensive R&D efforts.

Additionally, experienced IT system security developers entering the ICS protection market encounter new challenges, including the need to support outdated and highly specialized technologies, along with stricter industry regulatory requirements. It can also be difficult for them to accept that conventional corporate security approaches in the industrial sector simply do not work. To complicate things further, security experts and production engineers often "speak different languages" and struggle to understand each other's motivations.

Finally, economic feasibility plays a significant role for the vendors themselves. Solutions for industrial protection have slow returns on investment against high R&D costs and do not generate steady revenue like subscription products. This is simply not profitable for many companies, especially smaller ones.

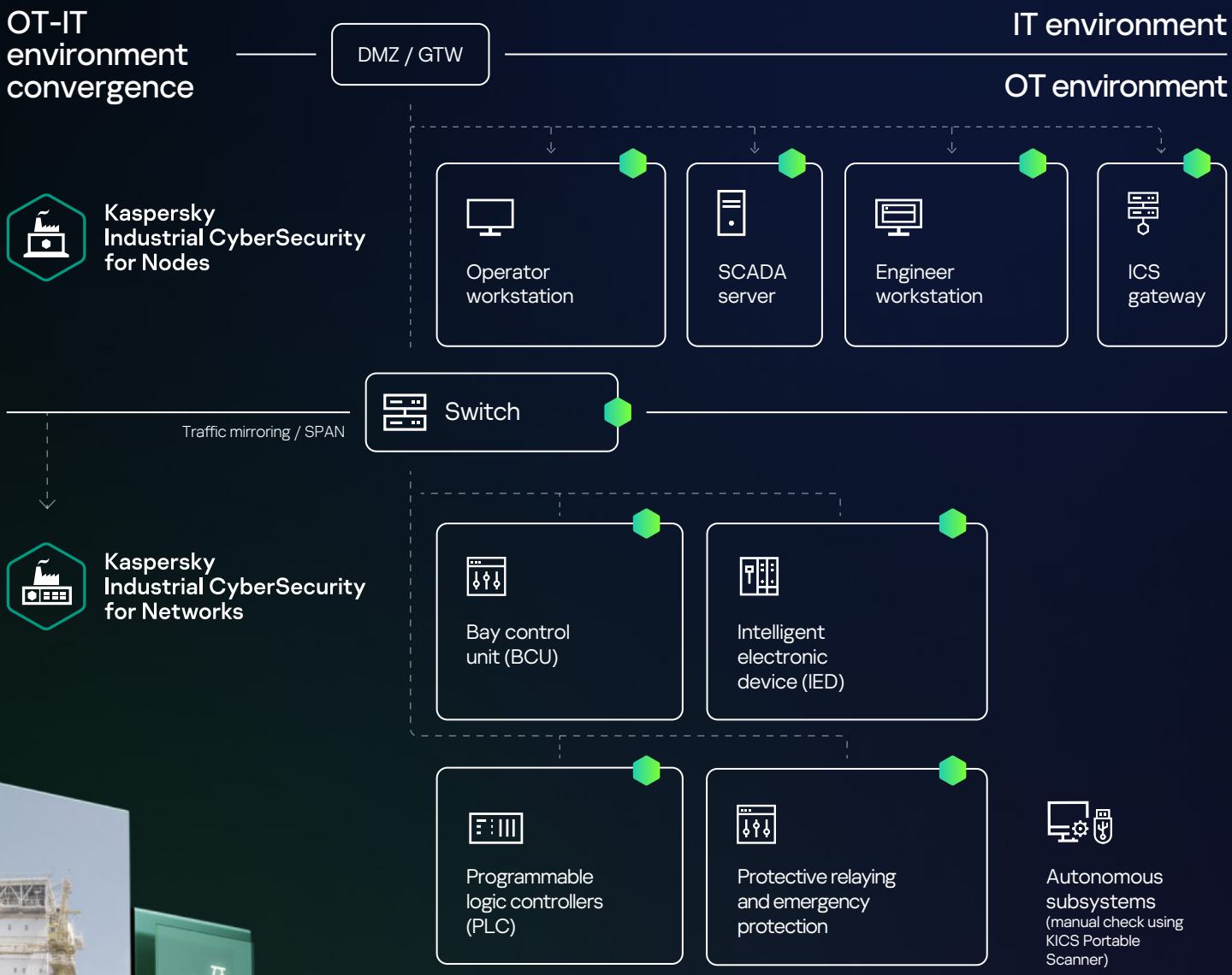
[6] See the report "Industrial Control Systems (ICS) Security Market size to cross $30 Bn by 2032" by Global Market Insights.

All of these efforts have allowed us to create a unified ecosystem of solutions for industrial corporations – Kaspersky OT Cybersecurity:



The core of this ecosystem is a set of solutions for protecting industrial networks, with the EDR solution Kaspersky Industrial CyberSecurity for Nodes being the most important component. This product, certified by government agencies of various countries, can be used to monitor and protect SCADA systems and verify the integrity of PLCs.

Platform usage points



Kaspersky Industrial CyberSecurity for Nodes is one of the two components of the Kaspersky Industrial CyberSecurity XDR platform. When combined with Kaspersky Industrial CyberSecurity for Networks, which analyzes industrial network traffic for threats, it functions as an endpoint sensor, providing complete XDR functionality. The platform holds the TÜV AUSTRIA certificate for compliance with the criteria of the IEC62443 4-1 secure development standard.

Kaspersky's process of building and updating antivirus databases has also been audited for compliance with international SOC 2 Type 1 requirements for protection against unauthorized changes.

Supplemented by other Kaspersky solutions and services for industrial information security, the Kaspersky Industrial CyberSecurity platform can provide multi-layered defense in depth.

Process	Corresponding functionality
Hardening the system by reducing the attack surface	· Device discovery for inventory purposes (Kaspersky Industrial CyberSecurity for Networks) · Wireless network control · Device control
Enabling available protection measures	· Advanced signature-based protection technologies · Cloud-based protection using the Kaspersky Security Network reputation database or the Kaspersky Private Security Network reputation database for isolated networks · Host-level firewall · Anti-Cryptor (protection against blockers and ransomware)
Continuous monitoring of the security of ICS, networks, and connections	· Monitoring launches of unauthorized software based on a list of allowed programs (can operate in both detection and blocking modes) · PLC integrity control · Wireless network control · Device control · Transmission of industrial network event data to other systems such as SIEM, MES, BI, and XDR
Managing ICS and technological network security based on risks	· Centralized security policy management (Kaspersky Security Center)
Human factor management	· Sending security incident notifications directly to operator panels · Logging potentially unsafe operator actions

Table 2. How Kaspersky Industrial CyberSecurity for Nodes supports the defense-in-depth approach (in combination with other Kaspersky solutions)

www.kaspersky.com

#kaspersky
#bringonthefuture