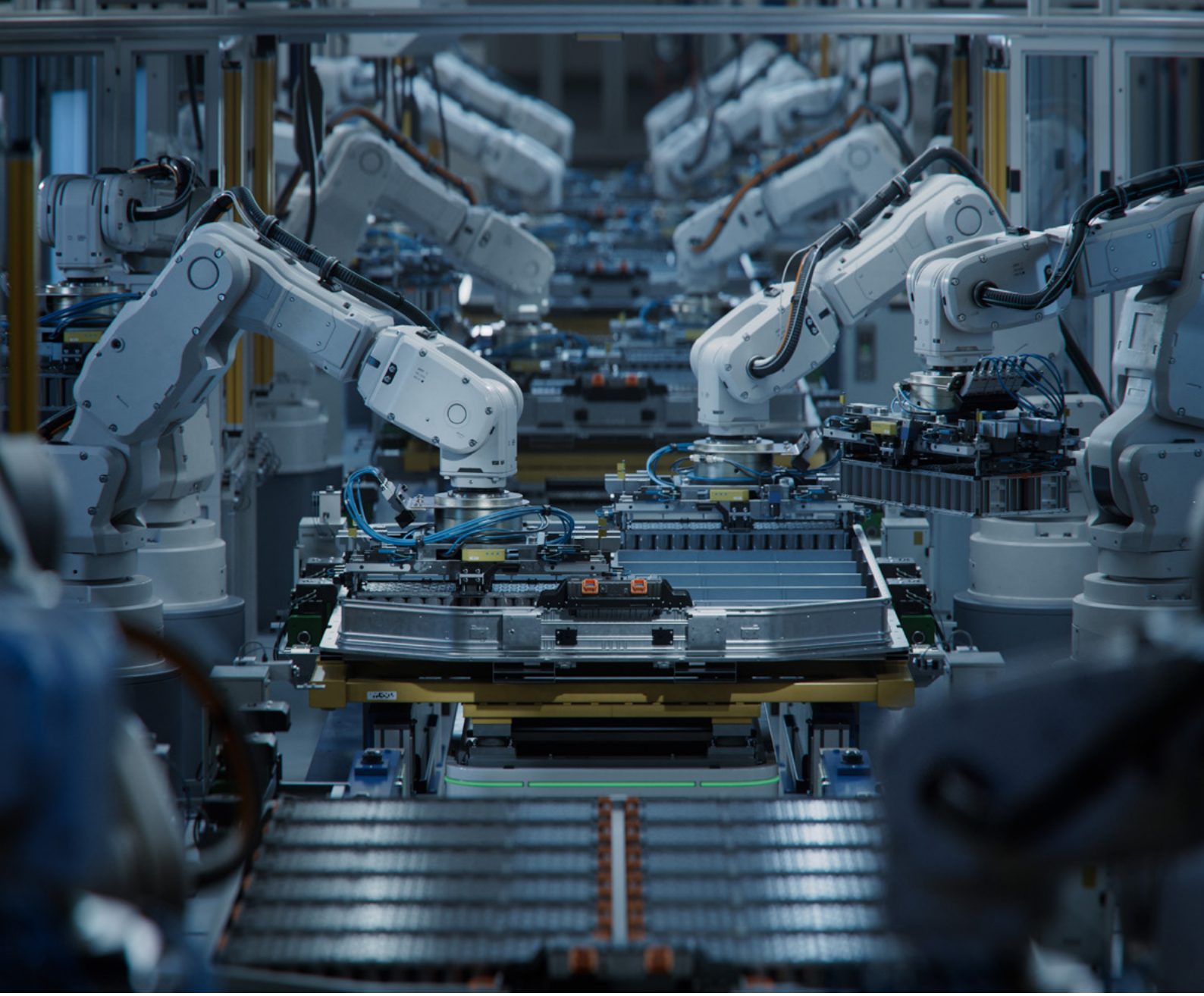


The State of Industrial Cybersecurity

Kaspersky's insights into Sector Threats

kaspersky.com
www.securelist.com

kaspersky BRING ON THE FUTURE

Introduction

The Fourth Industrial Revolution has brought forth unprecedented opportunities for innovation and economic growth, redefining industries globally. However, this new wave of technological advancement, while promising, also brings new risks and challenges.

Nowhere is this more evident than in the industrial cyber threat landscape. For some time now industrial sectors have been experiencing an alarming rise in cyber-related incidents. Even though the cybersecurity maturity of industrial enterprises is growing, their OT systems are still being exposed to cyberthreats[1]. These threats primarily affect systems that program, monitor and control increasingly interconnected industrial operations, from engineering workstations, 3d- and physical modelling and CAD/CAM systems to SCADA servers, HMIs and other kinds of OT-related computers.

The rapid deployment of 'smart' factory initiatives around the globe, designed to streamline and automate production, has further exacerbated the situation. As these connected technologies become an integral part of industrial operations, cyber risks grow in parallel. This issue has not gone unnoticed by global cybersecurity companies, such as Kaspersky, which has a vast network of threat intelligence experts who actively work with industries worldwide.

Critical infrastructure and manufacturing sectors have become prime targets for cybercriminals. One of the most significant incidents in recent history was the attack on Colonial Pipeline in May 2021[2]. The ransomware attack led to the shutdown of a major pipeline that supplies almost half of the US East Coast's fuel, leading to widespread panic, fuel shortages, and millions of dollars in damages.

Events such as this highlight the catastrophic consequences of cyberattacks on critical infrastructure: operational disruptions, financial losses, reputational damage, and threats to national security. These incidents underscore the importance of cybersecurity preparedness and response mechanisms within the industrial sector.

Drawing from its extensive experience in industrial cybersecurity, Kaspersky has explored the evolving nature of these threats and how they are perceived by the C-Suite – business leaders who are tasked with defending their companies from a host of cyberattacks. This report will discuss the findings from Kaspersky's research and outline the cybersecurity challenges facing industry today.

Methodology

Kaspersky conducted a comprehensive survey in August 2024, involving 406 C-level decision-makers from large enterprises with over 1,000+ employees in sectors such as energy, manufacturing, and oil & gas in the UK. The respondents were questioned about cybersecurity measures within their organisations, the barriers they face as management teams, and the challenges posed by vulnerabilities in their supply chains.

Key Findings

Cybersecurity awareness but insufficient preparedness

Despite widespread awareness, only 72% of respondents felt that their connected and automated supply chains were vulnerable to cyberattacks, with notable disparities between sectors:

- Oil & Gas: 81.90%
- Energy: 74.00%
- Manufacturing: 65.56%

Prevalence of cybersecurity incidents

A staggering 89.66% of organisations had experienced a cybersecurity incident in the last 12 months, with nearly half of these being classified as major disruptions:

1 Industrial sector attacks on the rise: an annual overview by Kaspersky
2 www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

- Energy: 95.33%
- Manufacturing: 88.08%
- Oil & Gas: 83.81%

IoT is perceived as the top cybersecurity threat

The survey revealed the primary cybersecurity threats perceived by industrial organisations:

- Connected/IoT device vulnerabilities – 20.94%
- Unauthorised access or credential theft – 17.98%
- DDoS attacks – 17.49%

"There's a mindset of 'security through obscurity,' where organisations believe that because their systems are not well-known or their vulnerabilities are hidden, they are less likely to be targeted," explains David Emm, Principal Security Researcher, Kaspersky. "However, this approach is flawed, as it relies on keeping details obscure rather than actively securing the system. In reality, this can create a false sense of safety, leaving critical Operational Technology (OT) environments vulnerable to sophisticated attacks."

Industrial Cybersecurity: A Snapshot

Regions across the globe are experiencing varying degrees of cybersecurity maturity for their industrial enterprises, but improvements in their cybersecurity culture and investments in protection measures have led to a decline of exposure of OT infrastructures to cyberthreats according to Evgeny Goncharov, head of Kaspersky's ICS CERT[3]. "Despite this, the overall risk remains high, as for the sophisticated actors even a small degree of exposure would be enough. And the things are getting more and more complicated as industries adopt smart technologies, which introduce new entry points for the attackrs as well as the new ways to propagate the attack to peer organizations."

"Ransomware continues to be a critical concern, with cybercriminals increasingly targeting industrial enterprises for financial gain. In parallel, hacktivism is on the rise, where politically motivated attackers are using ransomware tactics to disrupt industries and cause significant damage," says Goncharov.

Recent examples of high-profile cyberattacks underscore the potential financial losses industrial companies can face include Johnson Controls, a producer of building automation systems, which

3 Industrial cybersecurity in 2024: trends and forecasts

suffered a ransomware attack that resulted in a $30 million loss. Similarly, MKS Instruments, a chip manufacturer serving the automotive industry, faced $200 million in damages, while Clorox, a major producer of disinfectant products, saw its net sales take a $357 million hit due to production halts caused by a cyberattack. These incidents illustrate the devastating impact cyberattacks can have on companies, particularly when production and shipping operations are disrupted.

The rising threat of OT over IT

The industrial threat landscape for Q2 2024 highlights that cyberthreats are still affecting OT environments, including in energy and manufacturing sectors[4]. Key threats include ransomware, data theft, and malware propagation. The report reveals that malicious internet resources and phishing remain a common entry points for attackers. Sophisticated threat actors are also focusing on supply chain compromises to infiltrate targets. Enhanced cybersecurity measures are advised to protect these critical infrastructures.

As more industrial systems come to rely on interconnected devices, the risk of cyberattacks grows. Attackers recently exploited vulnerabilities in critical systems, such as a water supply system in Ireland causing operational disruptions[5].

The integration of telemetry and fleet management systems in vehicles further increases the potential for attackers to take control of their logistics, including transportation fleets. Remote energy and oil and gas facilities may also be vulnerable to a similar threat. With more industries adopting digital connected systems, the likelihood of large-scale cyberattacks with severe consequences is only expected to rise.

OT involves the management of physical processes and machinery, making it more susceptible to targeted cyberattacks with real-world consequences. Many organisations are struggling to secure their OT environments as they expand into automated and interconnected systems. This shift has exposed a significant gap in cybersecurity, with threats moving from IT domains to OT infrastructures, leaving critical industrial operations vulnerable to attack.

Condor Carpets faced this very challenge[6]. As a company managing multiple production facilities with a complex network of machines and automation systems, it recognised the need for a tailored industrial cybersecurity solution. Its existing IT protections were no longer sufficient to manage the growing OT network, which included more than 30 machines and process lines.

4 Threat landscape for industrial automation systems, Q2 2024
5 H2 2023 – a brief overview of main incidents in industrial cybersecurity
6 Condor Carpets: Securing operations with Kaspersky

Lacking full visibility into its OT environment, Through the implementation of Kaspersky Industrial CyberSecurity, Condor was able to gain critical insight into its OT network and identify potential vulnerabilities in its programmable logic controllers.

"As our operations expanded, we realized that our existing IT protections were no longer sufficient to manage our growing OT network, which now includes more than 30 machines and process lines," said Patrick de Haan, IT Manager, Condor Carpets. *"We faced significant challenges in gaining full visibility and control over our complex OT environment without disrupting our continuous production cycles. Managing legacy systems running on under-supported software was a critical concern—we needed a solution that ensured robust security without impairing functionality.*

Our OT network's complexity, involving specialized SCADA protocols like Modbus and OPC UA, meant that standard IT security solutions weren't adequate. Additionally, with our rapid expansion and acquisition of new facilities, we needed to standardize cybersecurity across all sites to maintain uniform security protocols. Resource efficiency was also paramount; we required an effective, manageable, and lean cybersecurity solution.

Implementing Kaspersky Industrial CyberSecurity provided us with critical insights into our OT environment and allowed us to identify potential vulnerabilities in our programmable logic controllers. Their solution addressed all our challenges—it gave us comprehensive visibility and control, managed our legacy systems effectively, and didn't disrupt our manufacturing workflows. Kaspersky's solutions have revolutionized our network and cybersecurity profile. We're confident in their ability to protect our complex operations now and into the future."

The main cybersecurity threats faced by manufacturing, energy and oil & gas

Connected/IoT device vulnerabilities	21%
Unauthorised access or credential theft (attackers gaining access to manufacturing systems or sensitive data by impersonating legit credentials)	18%
Distributed denial of service (DDoS) attacks	17%
Insider threats (employees, contractors, partners with malicious intent)	17%
Ransomware	16%
Phishing and social engineering attacks.	16%
Legacy system vulnerabilities	16%
Zero day exploits	16%
Physical security breaches (physical intrusions/tampering with equipment leading to cyber risks/disruptions)	15%
Supply chain attacks	15%
Malware and botnets	14 %
Regulatory non-compliance (failure to comply with industry-specific regulations)	14%
Lack of network visibility (i.e. the risk of not knowing about some machines in your infrastructure).	14%
Cyber espionage	13%
Lack of security awareness and training	11%
Data breaches	10%
N/A No threats in particular	0.00%
Not sure	0.00%

Growing Threats to IoT Devices

The increased use of IoT devices in industrial operations has expanded the attack surface, exposing these systems to greater risks. 21% of respondents ranked IoT vulnerabilities as their top concern, emphasising the urgency for robust IoT-specific security protocols. The vast number of connected devices complicates security efforts, as each device represents a potential entry point and often cannot be readily updated without disrupting operations. Addressing these risks requires a comprehensive approach, including continuous

monitoring, network segmentation, and strict patch management, to safeguard industrial environments from the growing threats associated with IoT vulnerabilities.

Human Factors Still Pose a Significant Risk

Insider threats and phishing remain persistent issues in the industrial sector, with 16% of respondents citing social engineering as a key concern. This highlights the need for stringent access controls and continuous monitoring of employee and contractor activities. Effective measures include implementing stringent access controls, regular employee training to recognize phishing attempts, and continuous monitoring of employee and contractor activities. By addressing these human-centric vulnerabilities, organizations can significantly reduce the risk posed by insider threats and social engineering, fostering a more resilient security posture across their operations.

Legacy Systems

Legacy systems, which are often difficult to patch and maintain, are particularly vulnerable to attacks. Since these legacy systems are frequently integrated into essential industrial processes, they are difficult to replace or modify without risking operational disruption. As a result, organizations may adopt short-term security fixes, which can create further complexities over time. This reliance on outdated technology underscores the pressing need for a strategic approach to upgrade or secure legacy systems in industrial environments, prioritizing resilience against emerging cyber threats.

DoS Attacks

Denial-of-Service (DDoS) attacks present a growing risk to industrial operations, with 17% of respondents expressing significant concern over their potential impact. These attacks overwhelm networks by flooding them with excessive traffic, disrupting essential services, and potentially halting production. In industrial environments, where continuous uptime is critical, a DDoS attack can lead to severe operational and financial consequences, including revenue losses, increased recovery costs, and damage to customer trust.

Vulnerability of supply chains

The vulnerability of supply chains remains a critical issue for industries. Despite significant investments in technology and infrastructure, 72% of respondents feel their supply chains are susceptible to cyberattacks. Sector-specific figures show even higher levels of concern in Oil & Gas (81.90%) and Energy (74%).

This high level of vulnerability is linked to the rapid

digital transformation within industrial operations. Previously air-gapped systems, which were disconnected from external networks for security reasons, have now been opened to facilitate better data sharing and integration.

Unfortunately, this has also opened the door to new cyber threats. Kaspersky research suggests that the move toward greater connectivity has not been matched with a commensurate investment in cybersecurity protections, leaving supply chains exposed.

Cybersecurity incidents: A recurring problem

Nearly 90% of respondents reported having experienced a cybersecurity incident in the last 12 months. For many industries, these incidents were not isolated but recurrent events. 95% of energy companies, for example, had been attacked, leading to significant operational disruptions and production downtime.

These numbers reflect a worrying trend: companies are bracing for cyberattacks rather than preventing them. Many organisations have resigned themselves to the inevitability of being breached, shifting their focus from prevention to incident response and damage control. This reactive approach, however, is not sustainable in the long run.

Emm continues, "Organisations and risk managers are finding the cost of insurance prohibitive. Many don't know what else to do. There's a black hole of misunderstanding. It's a real concern for them. They are worried, but they rely on IT to handle everything. It's like a ticking time bomb."

Barriers to effective cybersecurity

When asked about the barriers to achieving a comprehensive understanding of cybersecurity at the management level, respondents identified several key challenges:

- Jargon and confusing technical terms – 25%
- Difficulty quantifying risk – 25%
- Balancing compliance with operational objectives – 25%

Interestingly, budgetary restrictions, often cited as a significant issue in cybersecurity planning, were less of a concern in this study, with 20% of respondents citing it as a barrier – this is still a significant percentage, albeit the least concerning issue overall for respondents.

The main barriers to a full and extensive understanding of cybersecurity

The use of jargon/confusing terms	25%
Difficulty quantifying risk (e.g assessing impact of cyber incident on production uptime, revenue & reputation)	25%
Burden of ensuring compliance with industry-specific regulation while balancing operational objectives	25%
Lack of cybersecurity expertise and technical knowledge	24%
Complexity of interconnected industrial control systems and operational technology	24%
Difficulty keeping pace with rapidly evolving threat landscape	24%
Cultural and/or organisational barriers	22%
General lack of time	22%
Perceived low risk of cyberattack	22%
Budgetary restrictions	20%

Develop a proactive approach to cybersecurity

The industrial sector's journey through the Fourth Industrial Revolution is marked by both immense potential and significant cyber risk. With increasing connectivity comes greater vulnerability, and the consequences of inaction are already being felt.

The message is clear: industrial companies must move from a mindset of inevitability to one of prevention. By investing in the right tools, training, and threat intelligence, they can secure their operations, protect their supply chains, and ensure long-term resilience in the face of evolving cyber threats.

Emm concludes, "Our research finds that there is a clear grey area where security gets pushed towards

IT, but IT doesn't know how to effectively secure an OT environment. There's a lack of training, particularly in OT-specific cybersecurity and understanding the cyber risks involves which also speaks to a shortage of skill sets in the UK. Most people in OT are network engineers—they're good at production technology, but not at cybersecurity. OT is very specific."

With a wealth of industry sector-specific knowledge and expertise spanning 25 years protecting more than 400 million users and 240,000 companies worldwide, Kaspersky is in a unique position to educate and raise awareness around the very real threat posed by cybercriminals to the industrial sector.

Using its heritage of protecting organisations in the space, Kaspersky has an opportunity to lead an awareness campaign around how the increasing connectivity of industrial systems present not just to a new wave of innovation, but also a new era of cyber risks, and why up-to-the-minute threat intelligence and end-point security need to be a critical component for any modern manufacturing organisation's defence strategy.

Prevention over cure

Kaspersky's ethos centres on preventing attacks, rather than simply reacting after a breach occurs. The company recognises that while many vendors excel in incident detection and remediation, the real value lies in stopping cyberattacks in their tracks.

This proactive approach is especially critical in industrial environments where downtime can lead to significant financial and operational losses. According to Kaspersky data on average, it costs more than half a million US dollars to recover from a security breach for an enterprise. While the average expected loss for SMBs is $38,000 .

Kaspersky's solutions are designed to address the unique challenges faced by industrial operations, particularly in OT environments where security practices often lag behind those in IT.

Solutions for a safer industrial future

KICS (Kaspersky Industrial CyberSecurity)

OT and IT environments are becoming increasingly integrated, exposing systems to new cyberthreats and requiring a comprehensive single-vendor cybersecurity solution. To enable reliable protection of industrial networks and automation systems, use Kaspersky Industrial CyberSecurity (KICS), an OT XDR platform, offering centralized asset and risk management, security and compliance audit, unparalleled scalability and IT - OT Convergence with Kaspersky ecosystem.

Digital Footprint Intelligence

Kaspersky offers digital footprint intelligence to help organizations identify vulnerabilities and misconfigurations within their networks. This tool enables companies to understand where they are most exposed and take proactive measures to secure their infrastructure.

ICS Training and Upskilling

Kaspersky's Industrial Control Systems (ICS) cybersecurity training focuses on equipping employees with the knowledge and skills they need to respond effectively to cyber incidents. This is crucial as more industrial companies rely on IT teams to manage their OT security, which often leads to gaps in understanding and protection.

ICS Vulnerability Feed

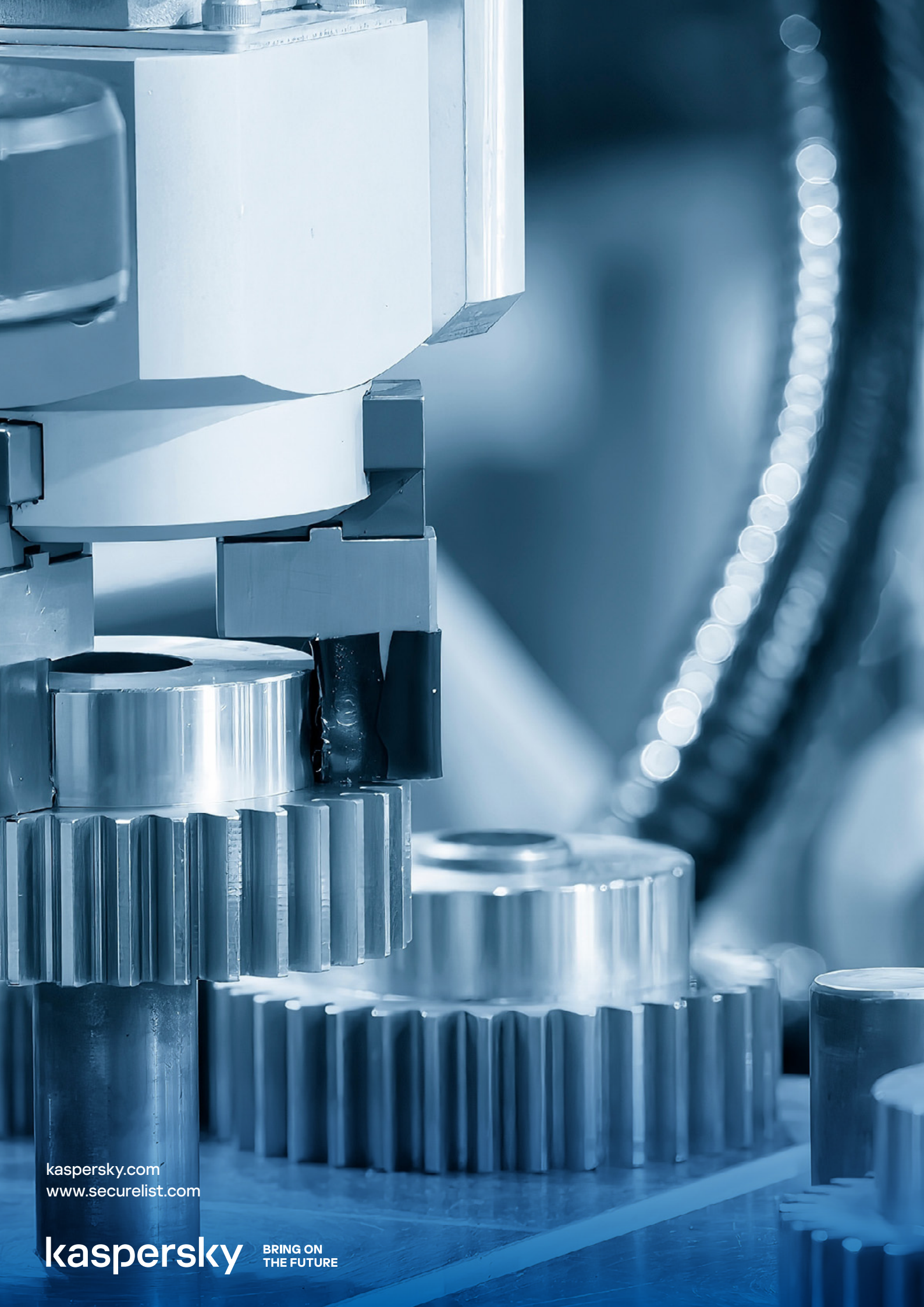
To address many challenges in patching OT vulnerabilities, Kaspersky provides real-time vulnerability feeds that help companies identify and patch weaknesses before they can be exploited.

ICS Threat Inelligence

To understand malicious actors tactics and to know which security weaknesses their victms had at the time of the attack that led to the infrastructure compromise and to better plan cybersecurity measures essential for keeping your organization protected.

Extended Detection and Response (XDR)

Kaspersky's XDR capabilities provide a comprehensive solution for detecting and responding to sophisticated threats like zero-day exploits and ransomware. This technology integrates threat intelligence with automated response mechanisms to help companies mitigate risks in real-time.



kaspersky.com
www.securelist.com

kaspersky BRING ON THE FUTURE