EXECUTIVE SUMMARY

KUDELSKI SECURITY

2024 Cybersecurity Trends and Actionable Insights

2024 Cybersecurity Trends and Actionable Insights: Executive Summary

This briefing highlights the most important findings from our 2024 Cybersecurity Trends and Actionable Insight report, including perspectives on the current state of cybersecurity, how trends will play out, and how organizations can address evolving risk.

The field of cybersecurity is undergoing rapid change. Methods that worked well in the past are no longer as effective. Today's cybersecurity teams face the challenge of expanding attack surfaces and of evolving threats, necessitating a shift in priorities and adapting their approach. Key areas of focus include heightened risk management, especially regarding third-party interactions, and the integration of automation and AI to bolster security measures. The adoption of Zero Trust frameworks is crucial for enhanced control over identities, and there is an increasing need for effective security incident response strategies. These elements together form the backbone of a robust and future-ready cybersecurity approach.

The vulnerability of the software supply chain represents a critical concern in cybersecurity. Recent years have seen a surge in supply chain attacks, highlighting the need for organizations to better understand and mitigate these risks. Developing and implementing robust security practices throughout the software supply chain is essential for resilience in 2024 and beyond. Additionally, traditional threats such as social engineering, ransomware, and insider threats continue to pose significant risks. Organizations must persist in investing in fundamental cyber hygiene and recovery capabilities to thwart these enduring threats and prevent avoidable incidents and breaches.

Furthermore, new regulations in various geographic regions are introducing additional complexities into the cybersecurity landscape. These regulations, which focus on cybersecurity, privacy, and AI, are shifting responsibility from end users to manufacturers, setting new disclosure requirements, and demanding enhanced cybersecurity risk programs.

Finally, the role of AI in cybersecurity, while still evolving, is undeniably significant and requires organizations to stay agile and prepared for rapid changes. This preparedness is also crucial in light of advancements in AI and quantum computing, which could potentially empower threat actors. Organizations must closely monitor these developments, particularly the fast-paced evolution of cryptographic technologies, to safeguard against the possibility of current data being compromised by future decryption capabilities.

The Cybersecurity Trends and Actionable Insights report is organized against 4 major categories with observations, perspectives and recommendations.

1. Strategic cybersecurity trends

2. Worldwide trends in cybersecurity

3. Trends in governance, regulation, and standards

4. Emerging threats

Strategic Cybersecurity Trends

Business and Cybersecurity Risk Convergence – Cyber risks have become inseparable from business risks. Crucial areas where cybersecurity and business risk management have converged are:

1. Third-party risk management
2. New cybersecurity and privacy regulations
3. Business continuity

To ensure organizations are positioned to respond to new and changing risks, there is a need for better understanding of cybersecurity risks by the C-level so they can understand and act on advice.

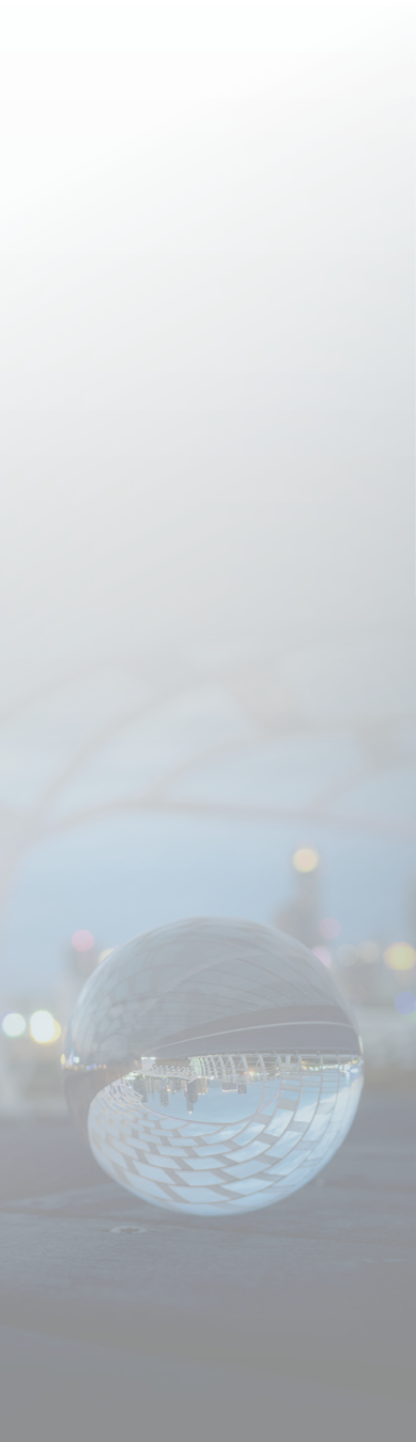
Rising Infrastructure Complexity – Modern IT architectures combine on-premise, cloud, OT, and more. To protect this architecture, organizations will need to invest in automation. Similarly, as the security perimeter has dissolved, many organizations have raced to adopt Zero Trust strategies, allowing them to continue with IT-based innovation while securing data and key business processes and protecting business continuity.

AI Benefits and Risks – AI has tremendous potential for adding business value but will also create new risks and threats that aren't yet known or understood. Early examples of these include prompt injection, data leakage, and AI-powered phishing. Organizations should develop an AI strategy as soon as possible to address the potential risks of AI as well as harness its benefits.

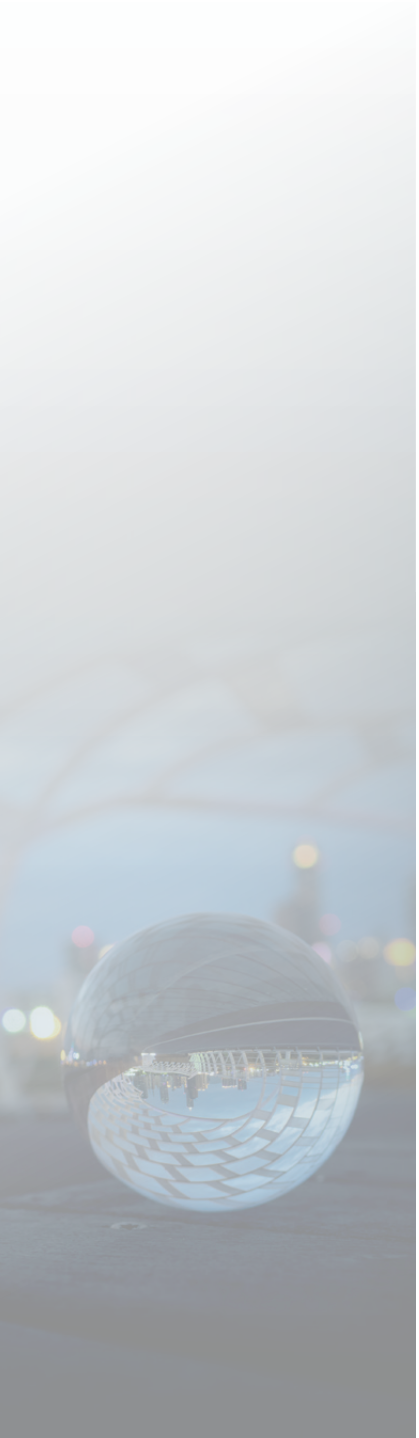
Building a Cybersecurity Culture – Technical controls are only part of the cybersecurity puzzle. Organizations must consider the role of humans in cyber defense. The main challenge is to ensure a consistent and up-to-date level of security awareness across an organization in a rapidly evolving threat landscape.

Optimizing Security Operations – As the cybersecurity landscape grows increasingly complex, it's tough for organizations to maintain core competencies in-house. Ideally, organizations should have a managed detection and response team on hand to help them monitor, detect, and respond to cybersecurity incidents.

Streamlining IT Infrastructure – Security architects face a tremendous challenge as they adapt to evolving technologies and integrate new practices in support of business goals, including modernizing old systems and simplifying operations for better data control. Adopting a Zero Trust strategy will be key and requires thorough updates in data and identity management to ensure secure, validated interactions.



Worldwide Trends in Cybersecurity



Supply Chain Issues Weaken Otherwise Robust Software – According to Lineaje, poor visibility of software dependencies creates an unsustainable cycle of vulnerability discovery and management, overwhelming an organization's ability to mitigate third-party risk. Moreover, security teams have little control over risky SaaS-to-SaaS connections, which in 2023 enabled a wave of telco attacks tied to bad vendor security hygiene.

Social Engineering Continues to Lure Victims – Cyber criminals continue to exploit fear, urgency, special occasions, and seasonal events (e.g., the tax season, shopping deals, etc.) to lure users. While email is the primary delivery channel, a study reveals that cybercriminals are increasingly focused on mobile devices and personal communication channels.

Ransomware Is Still Rampant – Until significant changes are made in security controls, control implementation, and international law, ransomware attacks will continue. A Check Point report noted 1 in every 10 organizations worldwide were hit by attempted ransomware attacks in 2023, surging 33% from previous year, while ransomware groups grow more agile, often exploiting new vulnerabilities as soon as they became public knowledge.

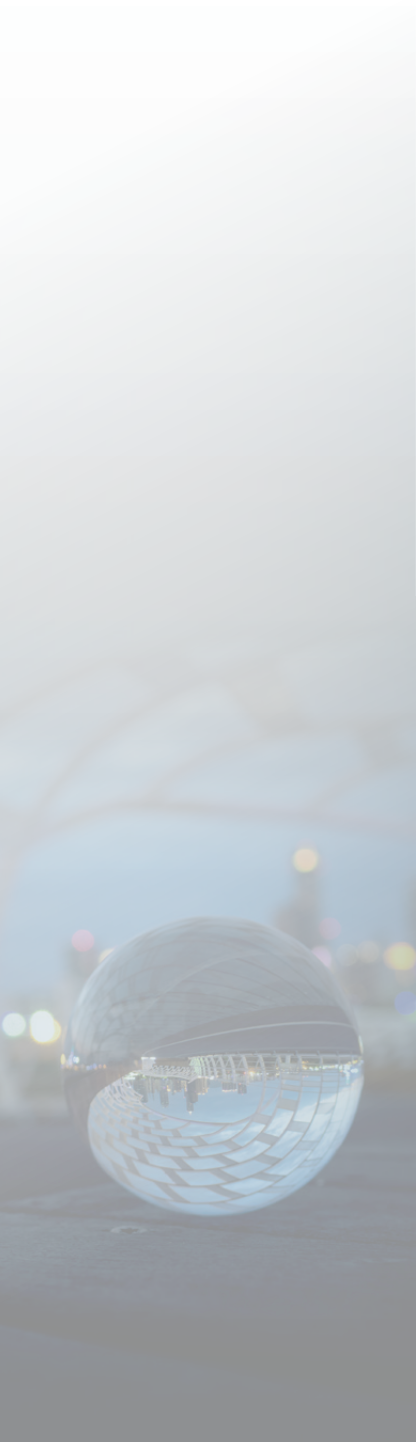
Geopolitical Tensions in Cyberspace – State-sponsored APT groups focus on long-term reconnaissance and crippling critical infrastructure of adversary nations. This dynamic will grow in complexity as countries amass cyber offensive capabilities to disrupt democratic societies, economies, and militaries. The implications are hard to predict—but this is a threat to all organizations, regardless of size or geographic location.

Insider Threats Continue to Thwart Cyber-Defense Efforts – Insider threats occur frequently and often go undetected. Insiders are “trusted” and therefore attract less scrutiny, with the result being greater access to systems—and greater harm from compromise. Since lax security practices are primarily responsible for insider compromises, they will continue until organizations strengthen controls.

Insights from Human Risk Intelligence Data Remain Largely Untapped – Inappropriate employee behavior is the number one cause of data breaches. However, only a small percentage of organizations use human risk intelligence in their risk scoring. Understanding human risk—including why and how decisions are made—is vital to implement appropriate security controls and prevent data breaches.

Cloud Security Continues to be a Challenge – According to research, the top security-related cloud threats are misconfiguration, data leakage, vulnerability exploits, and account compromise. Cloud environments have an overwhelming over-permissioning problem, with 99% of cloud users, roles, services, and resources granted excessive permissions that are ultimately left unused, according to Palo Alto Networks.

Trends in Governance, Regulation, and Standards



The Near Future of AI Regulation – Governments and regulatory bodies across the globe are rushing to regulate AI providers and companies who are building products that use AI technology. This includes the EU AI Act and the U.S. AI Act, which, once enacted, will significantly impact the use and development of AI products—e.g., by requiring organizations to explain AI models and their outputs in a way that makes sense to humans.

GDPR and New Privacy Laws – Navigating privacy laws will continue to challenge organizations, forcing them to prove compliance with complex requirements. Significant changes to the legislative landscape include:

- **Data privacy regulations' impact on AI.** Italy banning ChatGPT over privacy concerns was a wake-up call. The growing need to train generative AI models has led to companies scrambling for data, and many have changed user agreements and privacy policies to allow user data to be used to train AI models. This could prove a privacy risk and may be impacted by changing regulations.

- **New U.S. privacy regulations**. Multiple states have enacted consumer privacy regulations or begun to consider them, including California, Virginia, Colorado, Connecticut, and Utah. It's safe to assume these laws will be amended to include AI-specific provisions. Organizations must understand what data they hold, how it's used, collected, and stored, and which systems and users have access.

- **The White House cybersecurity push.** The new National Cybersecurity Strategy aims to ensure a safe digital environment and reshape cyberspace to reflect American values, including economic prosperity, human rights, democracy, and an equitable society. It reassigns roles, duties, and resources, shifting cybersecurity responsibilities from individuals to larger organizations.

- **The "U.S. Cyber Trust Mark".** The White House launched a cybersecurity certification initiative to help consumers identify secure smart devices, such as televisions, refrigerators, and fitness trackers. Key industry players like Amazon, Best Buy, Google, and Samsung have shown support, with products meeting the criteria being permitted to use the program's distinctive shield logo.

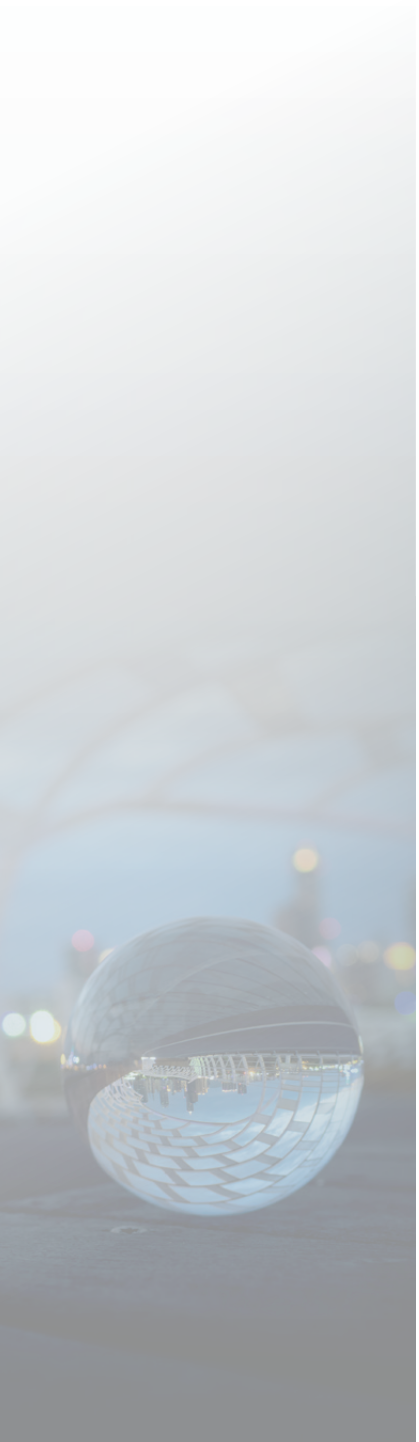
- **New SEC Rules.** The SEC has implemented new cybersecurity reporting and disclosure rules for U.S. organizations and foreign private issuers. Organizations must report serious incidents within four business days of detection and disclose risk management, strategy, and governance details in annual reports. These rules apply to reports for fiscal years ending December 15, 2023 onwards.

- **NIST releases CSF 2.0.** This framework, published in February 2024, expands the scope from critical infrastructure to all organizations, reflecting the broader remit with a new name: "The Cybersecurity Framework." NIST CSF 2.0 also introduces a new "govern" function alongside the existing five, emphasizing the importance of internal decision-making in cybersecurity strategy and highlighting cybersecurity as a key enterprise risk.

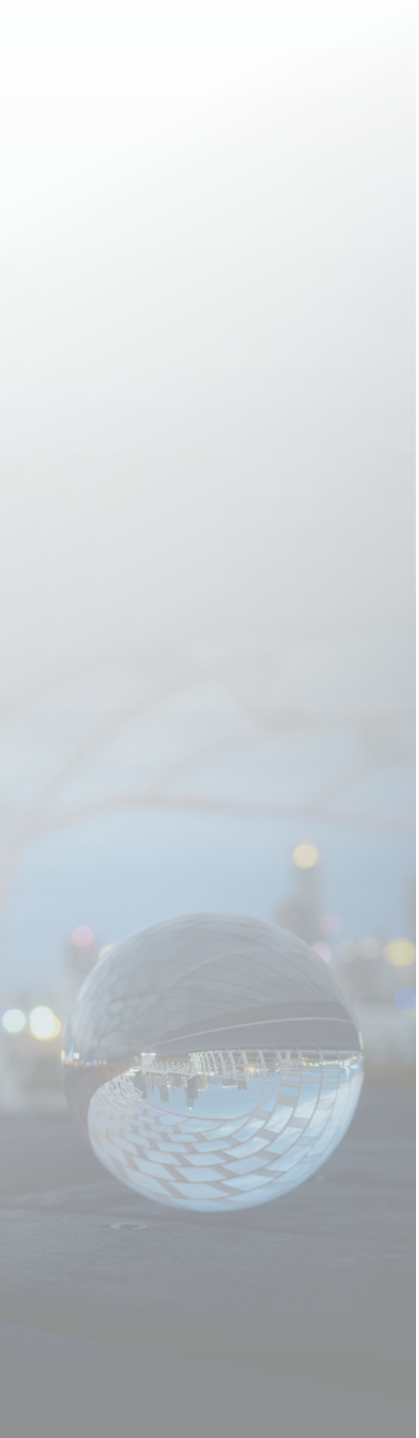
- **NIS2 entered into force in the EU** to strengthen digital products, protect customers, and ensure defensible critical infrastructure—particularly in vital sectors that rely on ICT, such as energy, transport, water, banking, financial markets, healthcare, and digital infrastructure. There will be significant penalties for non-compliance, as well as temporary suspension of C-Level executives and board members.

- **DORA launched in the EU** to ensure ICT infrastructure in the EU financial sector is adequately protected from cyber threats. The Act establishes cybersecurity standards that affected organizations and their third-party technology providers must implement by January 17, 2025. DORA also aims to harmonize existing ICT risk management regulations across EU member states.

- **Federal Act on Data Protection launched in Switzerland.** Enforced in September 2023, the (nFADP/LPD) can issue penalties of up to 250k CHF.



Emerging Threats



Artificial Intelligence Risks – AI-powered software may be susceptible to new risks and vulnerabilities, such as data poisoning attacks, where malicious actors introduce malicious data, causing systems to malfunction. These risks necessitate a heightened level of scrutiny, governance, and security.

Large Language Models (LLMs) in Software Engineering – Rapid adoption and lack of visibility make LLMs a source of risk. In 2024, expect to see these risks turn into high-profile incidents as hastily deployed applications fall victim to new threats. There are two primary use cases for LLMs in software engineering:

1. **Code development.** LLMs have produced code with known vulnerabilities, such as SQL Injection or weak cryptographic controls. LLM-powered coding tools could have serious implications for the software supply chain, as popular libraries and dependencies may have vulnerabilities introduced.

2. **Developing functionality.** LLMs are probabilistic, not deterministic, meaning outputs aren't guaranteed to be accurate. It may be tempting for developers to collapse multiple pieces of functionality into a single call to an LLM, but this is likely to compound the risk of errors.

Malicious Use of Generative AI – Generative AI reduces the friction of creating malicious content in multiple formats, including text, image, video, and audio. This has led to threat actors experimenting with these tools to conduct and refine cyber attacks. However, while some new threats are concerning, others are overhyped.

1. **Deepfakes** are falsified synthetic media (e.g., video or audio). Attackers can take a person's likeness and create content that appears to show them committing a crime. Or, they could depict a fictitious event, such as a terror attack. Deepfakes are already used in misinformation campaigns and could be used to undermine democracy and spread panic or resentment.

2. **Social engineering.** Attackers are using LLMs to create enticing phishing emails that include contextual information about the target. Tools such as WormGPT and FraudGPT, which automate the development of social engineering and phishing campaigns, are already sold on the dark web. There has also been a rise in the use of cloned voices for malicious purposes, including bypassing voiceprint authentication at financial institutions and for use in attacks against human targets.

3. **Malware Creation.** Much has been made of the use of generative AI tools to write malware. High-profile research projects have included the use of ChatGPT to create functional malware, further reinforcing these fears.

A deeper look at this research, however, shows that the malware produced is often in languages like Python or Golang—not primary languages for malware distribution.

4. **Upskilling inexperienced attackers.** It has been claimed that generative AI will "upskill" inexperienced attackers, allowing them to pose a greater threat. Fortunately, these fears are overblown. The Kudelski Security Research Team determined using generative AI tools effectively requires a level of sophistication, as well as the ability to identify and resolve errors in the resulting code.

Quantum Computing Advancements – A quantum computer capable of breaking today's encryption is drawing near. Businesses holding long-term confidential data must act now. NIST has concluded its process for defining new quantum-resistant standards, and organizations are expected to begin transitioning in 2024.

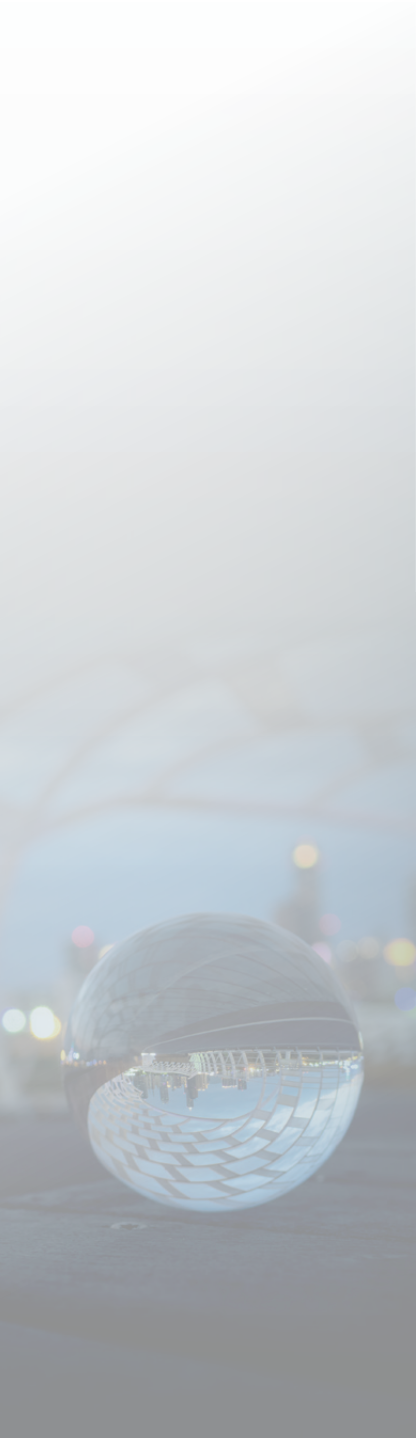
Acceleration of Cryptographic Technology – Cutting-edge cryptographic methods, such as zero-knowledge protocols and multiparty computation (MPC), promise enhanced security but introduce complexities and risks. Organizations must adapt with caution, auditing their cryptographic protocols rigorously to avoid vulnerabilities. Investing in specialized cryptography training for in-house teams is also a prudent step.

Digital Transformation of Critical Infrastructure – Critical infrastructure is a cornerstone of socio-economic prosperity. Implementing new technologies in a technologically reserved ecosystem has the potential for benefits—but poses new risks to organizations and society as a whole. Significant introductions include:

- **Drones** are used for crop monitoring, surveying sites, inspecting utility infrastructure, delivering goods, checking warehouse inventory, and more. This has opened these ecosystems to new threats. Drones are susceptible to interception, spoofing, and hijacking and may pose supply chain security issues.

- **IoT and edge computing** improve industrial processes via automation, on-device processing, and IIoT threat detection. However, as organizations deploy more devices, it will become harder to monitor them and ensure basic cyber hygiene, and they may strain bandwidth, slowing critical operations.

- **Cloud solutions** in OT environments are enabling much-needed agility, flexibility, and scalability. Again, this introduction poses challenges and risks. The cloud opens up the ecosystem to new cyber threats, misconfigurations, and supply chain issues that OT environments were once isolated from.



Read the Full Report

All of the events, trends, ideas, and predictions discussed here are covered in more detail in the full report along with recommended points of reflection and action.

DOWNLOAD THE 2024 TRENDS AND INSIGHTS REPORT

www.kudelskisecurity.com | info@kudelskisecurity.com

KUDELSKI SECURITY