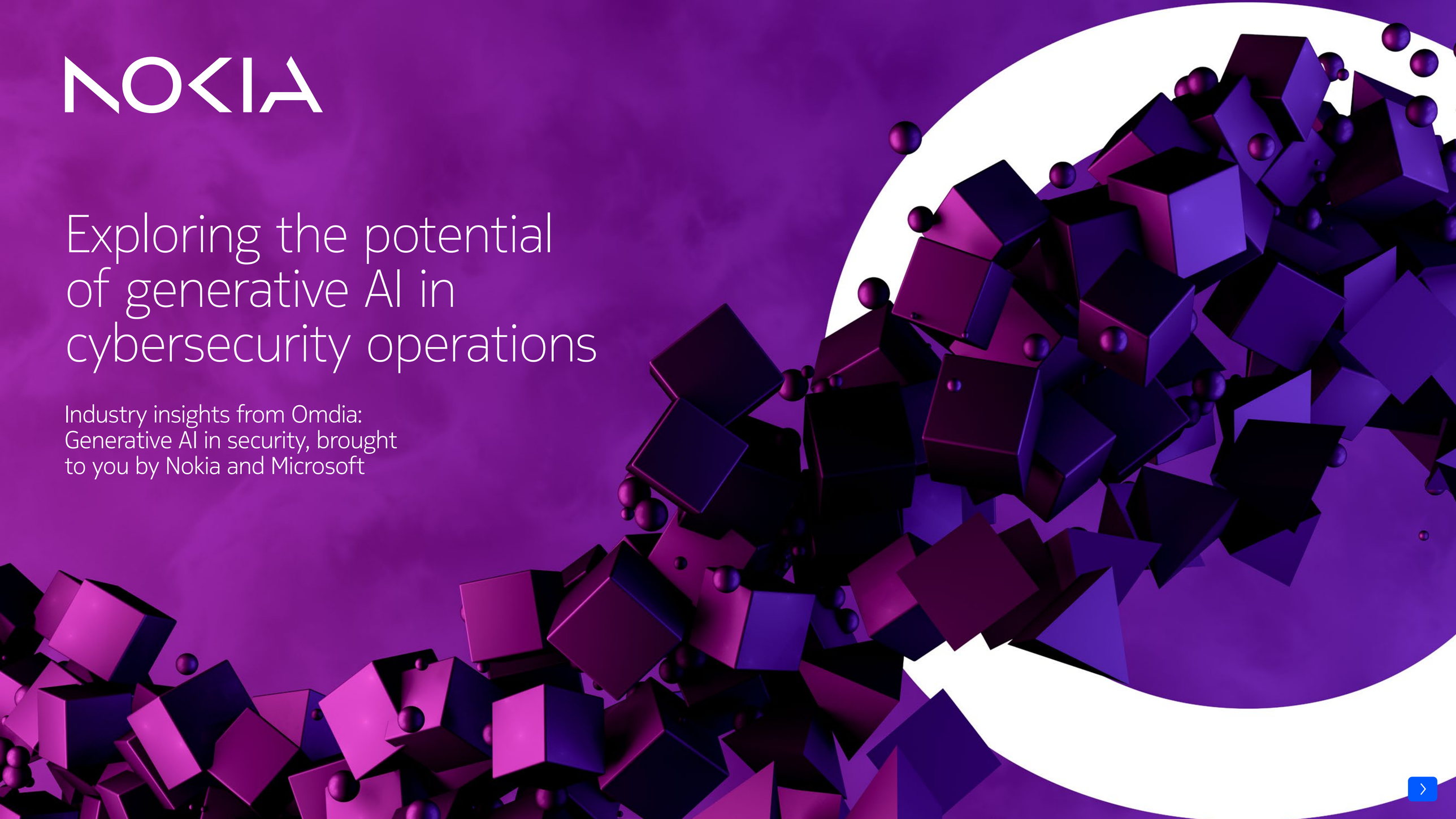
Exploring the potential of generative AI in cybersecurity operations

Industry insights from Omdia: Generative AI in security, brought to you by Nokia and Microsoft



The price of progress – is it worth the investment?

Traditional security measures are no longer enough in today's landscape of sophisticated cyber threats. AI has the potential to enhance cybersecurity by analyzing extensive datasets and identifying patterns. All of which are crucial for strengthening the cybersecurity posture. Generative AI stands out for its unique advantages in threat detection, incident response, and comprehensive security management.

Generative AI isn't just a tool; it's a game-changer. Imagine a world where security isn't just about reacting to threats but predicting them before they strike. Utilizing the advanced capacity of GPT, we have the capability to envision potential cyber-attacks and formulate defensive tactics within a virtual testing ground.

Through automated security incident handling, GenAI can revolutionize incident response and its ability to accurately replicate real-world data. A key advantage is how it can generate tailored actions based on the incident's nature. This enables security operators to automate initial response steps, swiftly address common threats, categorize incidents by severity, and suggest mitigation strategies – improving response times and accuracy. However, it's crucial to address concerning factors, such as data poisoning. This emphasizes the need for a well-rounded approach to AI-driven security solutions.

69% of mobile operator respondents said they have incorporated, or are in the process of incorporating, generative AI into their cybersecurity strategy.

Nokia and Microsoft commissioned Omdia report, 2024

GenAI vs GenAI - understanding how generative AI shapes cyber defense strategies

While GenAI's capabilities are undeniably impressive; its implications have sparked serious concerns among cybersecurity experts. The fear of potential misuse by malicious actors has sparked intense debates within the security community, forcing us to confront the profound security implications of this cutting-edge technology.

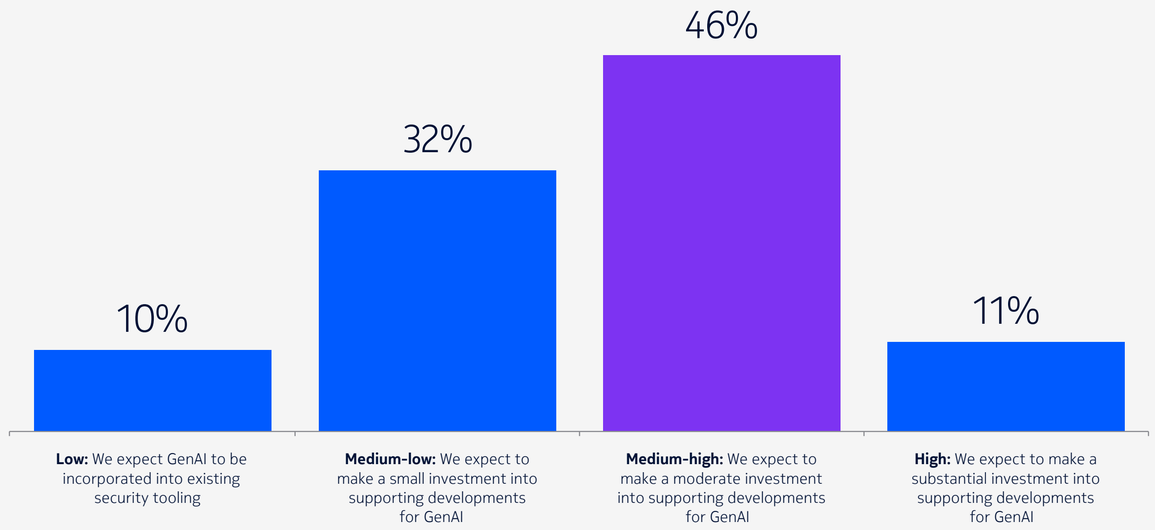
Generative AI and large language models (LLMs) can significantly expand the attack surface, empowering cybercriminals to automate the generation of sophisticated malware and orchestrate complex, multi-stage attacks with relative ease. Basic cyber threats, such as phishing attacks, can be executed with increased efficacy and minimal effort.

Amidst these challenges, there's a bright opportunity to leverage GenAI technology in cybersecurity. Within Security Operations Centers (SOCs), AI models play a pivotal role in identifying patterns that signal potential cyber threats, including malware, ransomware, and irregular network activity, that conventional detection systems might overlook.

With responsible AI usage and a commitment to ethical principles and data privacy, the power of these emerging technologies can craft innovative strategies that effectively combat emerging cyber threats.

In essence, while GenAI presents inherent risks, it also offers opportunities for proactive defense and resilience-building in the face of evolving cybersecurity challenges. With responsible AI usage and a commitment to data privacy, stakeholders across the landscape can collaborate and navigate these complexities to drive positive change in cybersecurity.

Figure 1. Question from Omdia Industry Insight Report 2024: How do you prioritize your cybersecurity budget in relation to adopting new technologies like GenAI?



Key benefits of integrating GenAI into cybersecurity strategies

Generative AI doesn't just simplify cybersecurity protocols – it's similar to a digital assistant that can take care of mundane tasks and provide next steps, leaving cybersecurity teams free to tackle complex issues.

One key benefit of GenAI is enhanced threat detection and response. This emerging technology can craft intricate models that forecast and pinpoint anomalous patterns that are consistent with cyber threats. This empowers security systems to react swiftly and decisively, outpacing conventional approaches.

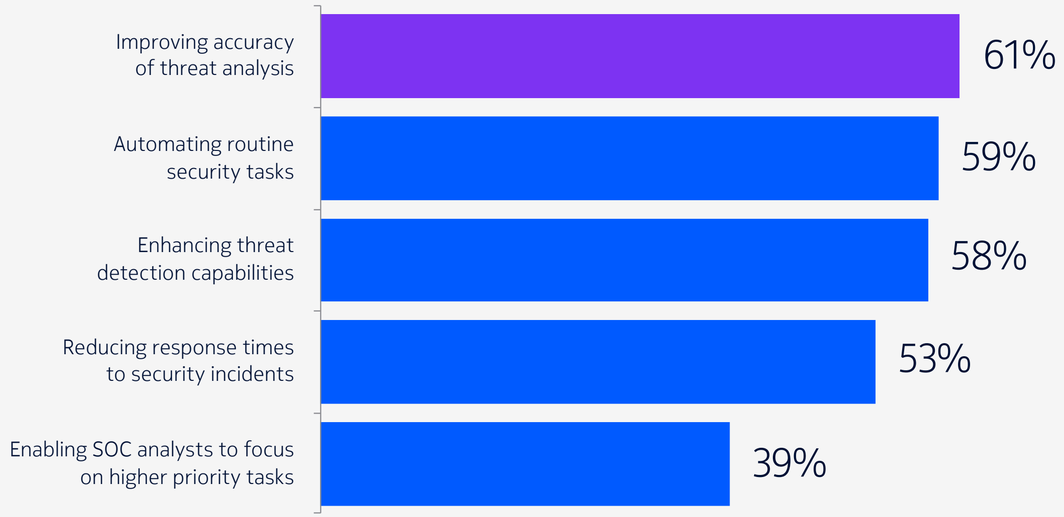
By constantly learning from data, generative AI keeps up with new threats, reducing the chances of breaches and lessening their impact if they occur. Security teams benefit from detailed insights into how threats work. This helps them plan targeted responses and strengthen their defenses against future attacks.

Another key benefit of GenAI is automating and streamlining security operations. This frees up human resources to focus on tackling more intricate challenges and reduces the risk of human error. Additionally, security protocols can be tailored by analyzing extensive data to predict and implement the most efficient measures for specific threat scenarios.

Consequently, organizations can implement flexible security solutions that scale with their needs and adapt to evolving threat environments.

Figure 2. Question from Omdia Industry Insight Report 2024: What potential benefits do you see in integrating GenAI into your cybersecurity operations?

Respondents perceive several potential benefits of integrating GenAI into cybersecurity operations, including improved accuracy of threat analysis (61%), automating routine security tasks (59%), enhancing threat detection capabilities (58%), and reducing response times to security incidents (53%).



GenAI's impactful applications in cybersecurity

Generative AI has many applications in cybersecurity operations. It helps us stay safe online by spotting problems early and strengthening our defenses every day.

Automating incident response not only saves time and costs but also enhances overall security posture by containing the affected systems in real-time.

Another application of GenAI in cybersecurity operations is through behavior analysis and anomaly detection which are vital cybersecurity techniques used to identify potential threats.

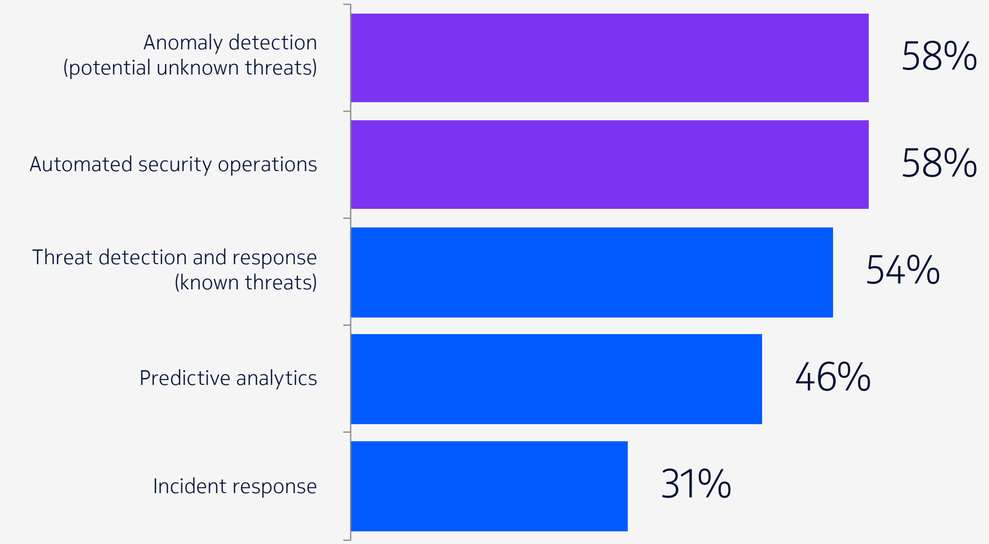
GenAI can take security to the next level by generating synthetic data of typical user or network behavior and detecting deviations from the norm.

Any deviations or anomalies may signal a security breach or unauthorized system access. By scrutinizing these anomalies and contrasting them with expected behavior patterns, security professionals can discern potential threats and take appropriate preventative actions.

Figure 3. Question from Omdia Industry Insight Report 2024: In which areas of cybersecurity have you applied GenAI?

The most common current applications of GenAI in cybersecurity strategy and operations include:

- Anomaly detection
- Automated security operations
- Threat detection and response



Navigating the risks – GenAI's impact on the cybersecurity landscape

Generative AI introduces both promising advancements and significant risks in the realm of cybersecurity. However, insufficient understanding of its benefits remains the top deterrent to its widespread incorporation into security strategies.

Cybercriminals may leverage generative AI to automate the creation of sophisticated malware, evade detection systems, or launch targeted attacks with unprecedented precision. As this technology matures, hackers will increasingly exploit its capabilities for malicious purposes, while bad actors refine their strategies to leverage this technology to their advantage. Security vendors must, therefore, expedite the enhancement of their products' capabilities to effectively address emerging threats. Pairing GenAI with human security expertise can help level the playing field and strengthen defense strategies against evolving cyber threats.

Moreover, the prospect of data poisoning poses an additional concern. Maliciously crafted inputs could corrupt the training process of GenAI models, leading to compromised security measures. Adopting robust security measures is essential for the safe deployment of GenAI/LLMs in CSPs and enterprises.

Examples of security measures for safe GenAI/LLM deployment:

- Sanitizing training data to prevent leaks
- Implementing strong user authentication
- Filtering outputs to ensure content safety

By prioritizing security measures and best practices, CSPs and enterprises can leverage GenAI's full potential while safeguarding against cyber risks, enabling an advanced, innovative, and more secure digital future.

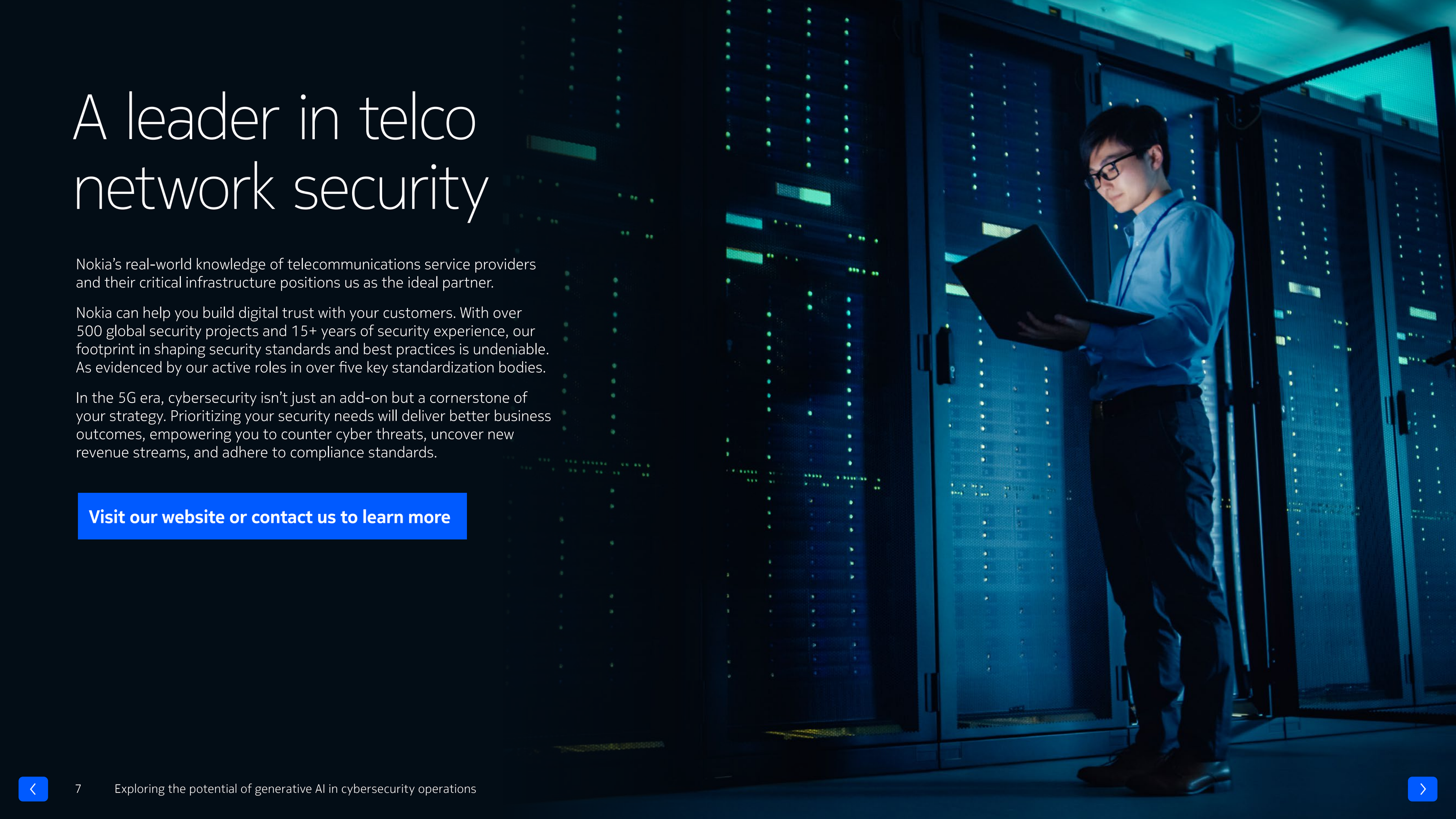
A leader in telco network security

Nokia's real-world knowledge of telecommunications service providers and their critical infrastructure positions us as the ideal partner.

Nokia can help you build digital trust with your customers. With over 500 global security projects and 15+ years of security experience, our footprint in shaping security standards and best practices is undeniable. As evidenced by our active roles in over five key standardization bodies.

In the 5G era, cybersecurity isn't just an add-on but a cornerstone of your strategy. Prioritizing your security needs will deliver better business outcomes, empowering you to counter cyber threats, uncover new revenue streams, and adhere to compliance standards.

Visit our website or contact us to learn more



Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214050 (June)

nokia.com

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.