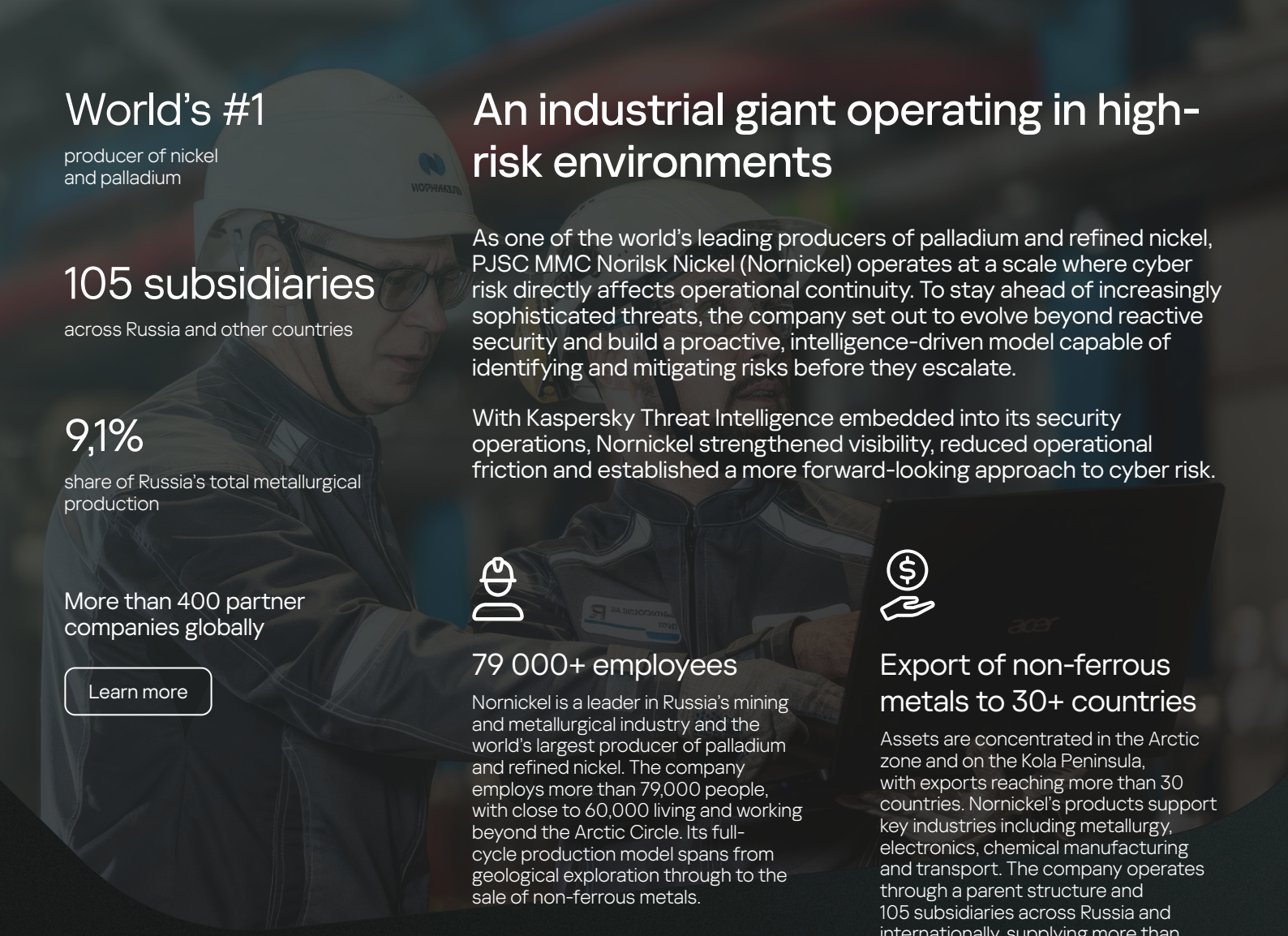
Cybersecurity transformation at PJSC Nornickel

From reactive defense to proactive risk control

kaspersky cybersecurity true to business

NORNICKEL



World's #1

producer of nickel and palladium

105 subsidiaries

across Russia and other countries

9,1%

share of Russia's total metallurgical production

More than 400 partner companies globally

Learn more

An industrial giant operating in high-risk environments

As one of the world's leading producers of palladium and refined nickel, PJSC MMC Norilsk Nickel (Nornickel) operates at a scale where cyber risk directly affects operational continuity. To stay ahead of increasingly sophisticated threats, the company set out to evolve beyond reactive security and build a proactive, intelligence-driven model capable of identifying and mitigating risks before they escalate.

With Kaspersky Threat Intelligence embedded into its security operations, Nornickel strengthened visibility, reduced operational friction and established a more forward-looking approach to cyber risk.

79 000+ employees

Nornickel is a leader in Russia's mining and metallurgical industry and the world's largest producer of palladium and refined nickel. The company employs more than 79,000 people, with close to 60,000 living and working beyond the Arctic Circle. Its full-cycle production model spans from geological exploration through to the sale of non-ferrous metals.

Export of non-ferrous metals to 30+ countries

Assets are concentrated in the Arctic zone and on the Kola Peninsula, with exports reaching more than 30 countries. Nornickel's products support key industries including metallurgy, electronics, chemical manufacturing and transport. The company operates through a parent structure and 105 subsidiaries across Russia and internationally, supplying more than 400 partner companies worldwide. more than 79,000 people, with close to 60,000 living and working beyond the Arctic Circle. Its full-cycle production model spans from geological exploration through to the sale of non-ferrous metals.

Long-term partnership

To support this shift, Nornickel expanded its long-standing partnership with Kaspersky – which had been formalized in 2017 through a strategic agreement aimed at strengthening information security across domestic industries.

The turning point: Recognizing the limits of reactive security

As cyberthreats grew more targeted and coordinated, Nornickel recognized that traditional reactive defenses were no longer sufficient for the scale and complexity of its operations.

The company set a clear objective: move to proactive protection capable of identifying risks before they developed into incidents.

Several factors made this shift urgent.

Publicly available corporate information had become an expanding attack surface. Even neutral data such as employee contacts, email address structures and interviews with senior executives could be weaponized for phishing, social engineering and "fake boss" attacks, particularly as deepfake technologies advanced. Nornickel needed deeper analysis of open-source intelligence alongside internal vulnerability data to model realistic attack scenarios.

At the same time, increased activity on the dark web raised the risk profile. Threat actors were coordinating and discussing actions targeting Russian companies. Nornickel required continuous monitoring of company mentions and broader visibility into risks affecting service providers, suppliers and partners, where compromise could cascade into the supply chain.

Internally, cybersecurity operations also needed to evolve. The security team was heavily engaged in ongoing risk discovery and user communications, operating largely within a restrictive, prohibition-focused model. Nornickel aimed to adopt a more business-oriented approach that would both strengthen protection and help employees better navigate cyber risks.

The strategy: Building intelligence into daily security operations

Nornickel's decision to use Kaspersky was the result of long-term collaboration. Over time, the company's cybersecurity team had the opportunity to test almost the full Kaspersky portfolio and implement the majority of the solutions within its environment. This hands-on experience gave the company a clear understanding of how Kaspersky products address real-world challenges in the manufacturing sector and operate effectively within complex industrial infrastructure.

Kaspersky's flexibility was also an important factor. As Nornickel noted, "Kaspersky sees us as a reliable partner with a mature approach to cybersecurity and listens to our needs for product refinement." This partnership model made it possible to integrate cyber intelligence directly into SOC workloads and use the services not as standalone tools, but as part of a unified, proactive security system.

Kaspersky Threat Intelligence

To gain visibility into threats at every stage of their progression, Nornickel deployed Kaspersky Threat intelligence as a core component of its proactive strategy.

Unified threat visibility with the Threat Intelligence Portal

Kaspersky Threat Intelligence Portal

At the center of the ecosystem is the Kaspersky Threat intelligence Portal, a unified environment that allows administrators to analyze malicious files, review expert reporting and access global threat landscape insights.

This enabled Nornickel to:

- Enrich alerts with meaningful context
- Prioritize incidents by criticality and scope
- Attribute activity to known threat actors
- Disrupt attacks at early stages before infrastructure entrenchment

Reducing exposure across the digital footprint

Kaspersky Digital Footprint Intelligence

To tackle risks linked to publicly available information and dark web activity, Nornickel implemented Kaspersky Digital Footprint Intelligence.

The solution provides digital footprint management, identifies potential data leaks and monitors mentions of the company and its employees in underground environments. By actively searching for vulnerabilities in web resources and mapping connections between corporate data and potential attack vectors, Nornickel strengthened risk management and removed non-essential information from open access.

Alexander Ardakov

Head of Practical Cybersecurity,
PJSC MMC Norilsk Nickel

Kaspersky Digital Footprint Intelligence lets us understand what information about the company is available to cybercriminals and how it can be used in attacks.

Faster, cleaner detection with Threat Data Feeds and CyberTrace

Kaspersky Threat Data Feeds + **Kaspersky CyberTrace**

To further enhance detection, Nornickel integrated Kaspersky Threat Data Feeds with Kaspersky CyberTrace within its existing security stack.

Threat Data Feeds deliver continuously updated indicators of compromise, while CyberTrace simplifies feed delivery to SIEM, NGFW and SOAR platforms and accelerates interpretation.

As a result, Nornickel achieved:

- Reduced false positives in detection systems
- Lower SOC engineer workload
- Greater focus on active threat protection

The outcome:
Stronger control, earlier risk reduction

Nhrough close cooperation with Kaspersky, Nornickel established more structured and controlled risk management procedures. The company gained earlier visibility into existing threats, improved its ability to assess defensive posture and prioritized vulnerabilities based on severity.

Operational impact:

More efficient SOC workload management

Deeper use of cyber intelligence in daily operations

Earlier-stage prevention of potential attacks

Organizational impact:

More mature dialogue with corporate users on digital hygiene

Increased trust in the internal cybersecurity team

Greater use of third-party leak and account exposure data

Why this matters:
Security that supports industrial resilience

For large industrial enterprises, cybersecurity is inseparable from production stability, supply chain integrity and corporate trust.

By embedding threat intelligence into daily operations, Nornickel transformed cybersecurity into a proactive, integrated capability aligned with business priorities. The result is a more resilient security posture that supports operational continuity and long-term risk management.

Kaspersky Threat Intelligence

Learn more

www.kaspersky.com

#kaspersky
#truetobusiness