Cybersecurity in a changing Europe

Why AI-augmented security is no longer optional and **why it does not have to cost a fortune**

nextgen
CYBERQUEST
NETALERT

A Nextgen Software
Market Perspective
Hani Darouich, CISSP

March 2026 © nextgensoftware.eu

Table of contents

The landscape has shifted. Permanently.

This is not a document about fear. It is a document about **clarity**. The organizations that will navigate this environment successfully are the ones making informed, level-headed decisions about where to invest, what to prioritize and which partners to trust.

European organizations face a set of pressures that, even two years ago, would have seemed unlikely to arrive all at once. **The threat landscape has intensified sharply. Regulatory obligations have expanded with real enforcement behind them.** The cybersecurity workforce is shrinking, not growing. And the broader economy is squeezing budgets at precisely the moment when investment in security matters most.

IBM's 2025 Cost of a Data Breach Report found that **organizations using AI extensively in their security operations save $1.9 million per breach** on average and **resolve incidents 80 days faster**. That is a compelling number. But it needs context, because the same report and others like it, also show that **AI adoption without proper governance introduces its own risks**.

As we explored in our earlier paper, **AI is both the Cure and the Disease**, the technologies strengthening defenses are simultaneously fueling new attack methods. CrowdStrike's 2026 Global Threat Report documented an **89% increase in AI-enabled adversary attacks. ENISA found that AI-supported phishing now accounts for over 80% of social engineering globally.**

What follows is our honest reading of where Europe stands, what is changing, and why we believe Nextgen Software's approach is the right answer for the organizations that need it most.

SECTION 1
The case for Agentic AI in Security Operations

Every major cybersecurity vendor shipped agentic AI capabilities in 2025. CrowdStrike, Microsoft, Palo Alto Networks, Splunk, they have all moved. The data behind the shift is solid. IBM found that **heavy AI users pay $3.62 million per breach versus $5.52 million for non-users**.

Gartner's data shows **AI-powered platforms cut mean time to respond by 84%.**

The financial argument is settled. What is not settled is who actually benefits from it.

The vendors leading this conversation are overwhelmingly American and their pricing reflects it. **Platform licensing alone runs €200,000 to €500,000 a year before professional services, integration, and the multi-year lock-in**. For a Fortune 500, that is manageable. **For a European mid-market company or an SME navigating NIS2 on a realistic budget, it is a barrier.**

And even with that spend, the model is struggling. SOC teams routinely **miss up to 30% of incoming alerts**. Analyst **burnout drives 25%+** annual churn. Gartner places AI SOC agents at the Peak of Inflated Expectations, and **72% of CIOs report breaking even or losing money on AI investments**. The hype is real. So is the gap between a polished demo and a Tuesday morning in your SOC.

30%

incoming alerts
missed

25%+

annual
analyst churn

72%

breaking even or losing
money on AI investments

Where Nextgen Software sits in this picture

> “Nimble where the giants are bloated. Responsive where they are rigid. Priced for the reality of European business.”

CYBERQUEST **was not built by bolting AI onto a legacy platform**. **It was architected from the start with agentic capabilities woven into its core.** The full data lake feeds into investigative agents that build context, correlate events across the kill chain and surface detailed remediation guidance. Every output is grounded in expert-curated detection logic and human-validated decision points. No hallucinated verdicts. No autonomous actions without oversight. The AI extends the analyst’s reach. The analyst remains the authority.

Paired with **NETALERT NDR**, **CYBERQUEST** delivers **SIEM** and **network detection capabilities** that compete directly with platforms costing five to ten times more. **Built in Europe, for European organizations**, by engineers who understand that a 200-person manufacturer in Wroclaw or a fintech in Bucharest **should not need Silicon Valley budgets to achieve serious security outcomes.**

SECTION 2
Economic and geopolitical pressures are reshaping priorities

Every euro spent on security competes with payroll, energy bills and the dozen other pressures European leaders are already managing. The ECB’s March 2026 projections revised **Eurozone GDP growth down to 0.9%, weighed down by the energy shock from the Iran conflict.** Gas storage across Europe stood at just 29% of capacity in mid-March. Industrial electricity prices already ran at more than double US and Chinese levels throughout H1 2025. The European Commission has introduced emergency energy price relief measures and EU leaders openly acknowledge that **energy costs are undermining competitiveness.**

US trade policy is compounding the pressure. A 15% universal tariff imposed in February 2026 has disrupted EU-US trade negotiations, with the European Parliament preparing retaliatory measures on €93 billion of US goods. For SMEs, the picture is particularly challenging: the **SME united Business Climate Index sits at just 70.6, barely above the recession threshold** and a **€400 billion financing gap constrains access to capital**.

Central and Eastern Europe: Growth despite the headwinds

Against this backdrop, Central and Eastern European economies continue to **outperform**. **Poland projects 3.5% GDP growth** in 2026, supported by substantial EU fund absorption and rising real wages. **Lithuania follows at 3.0%, with the Czech Republic at 1.9 to 2.4%**. The region's digital transformation is accelerating, with **software and IT spending expected to grow 50% by end of 2026 and nearly double by 2030.**

Defense and cybersecurity investment is reinforcing the momentum. Poland spends 4.7% of GDP on defence with $700 million earmarked for cybersecurity. The Baltic states have pledged to reach the 5% NATO target by 2026 with explicit cyber components.
The EU's ReArm Europe framework includes a dedicated €3.5 billion cybersecurity fund.

These are economies that think carefully about **value for money, that are digitising rapidly and that need security platforms built for their reality**. Not repriced American enterprise solutions with a localisation layer on top, **but purpose-built European technology**.

CYBERQUEST and NETALERT were engineered precisely for this market: **serious capability, sensible cost, deployed** and supported by a **team that understands both the regulatory landscape and the operational realities** of doing business in this part of Europe.

SECTION 3 - Compliance is no longer optional. The penalties prove it.

NIS2 compliance costs €50,000 to €300,000 depending on maturity.

The average breach costs **$4.44 million**.

One in five SMEs that suffered a cyberattack in 2024-2025 filed for bankruptcy, per Mastercard research.

"The market does **not** need another €500,000 annual platform. **It needs CYBERQUEST**."

NIS2, DORA, intensifying GDPR enforcement and the upcoming Cyber Resilience Act (September 2026) have collectively shifted cybersecurity from discretionary spending to **legal obligation**. For many mid-market companies and SMEs, particularly those newly in scope under NIS2's expansion from 7 to 18 sectors, this is **unfamiliar territory**.

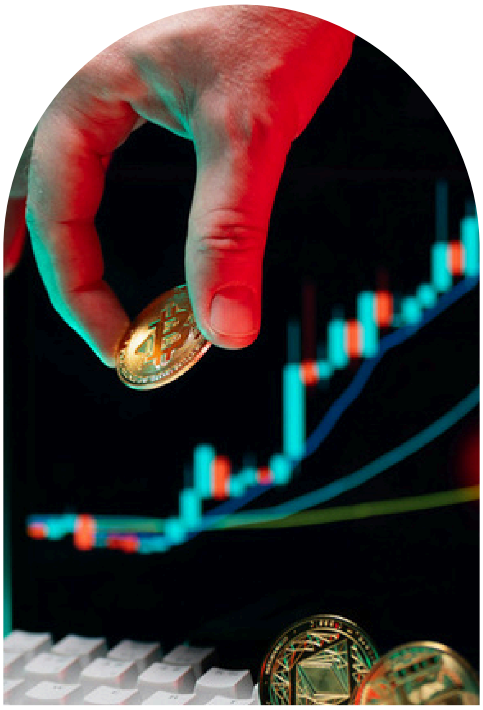
The penalties are substantial

Essential entities face **fines of up to €10 million or 2% of global turnove**r. Important entities face **€7 million or 1.4%**.

NIS2 Article 32 introduces personal management liability for gross negligence, including temporary bans from board positions.

DORA, applicable since January 2025, imposes additional ICT resilience requirements on financial entities with **penalties reaching 2% of worldwide turnover.**

GDPR fines hit €1.2 billion in 2024 alone, with enforcement broadening well beyond Big Tech into mid-market companies across all sectors.



SECTION 4 - The threat landscape demands continuous, intelligent detection

Three dynamics are compounding: the **cyber dimension of the Iran conflict, persistent Russian hybrid operations** and the **industrialization of ransomware** targeting European businesses. Each one alone would warrant investment in detection and response. Together, they create an environment where organizations without continuous monitoring are **carrying risk they may not fully appreciate**.

The US-Israeli strikes on Iran in late February 2026 **triggered immediate cyber retaliation**. Over 60 hacktivist groups mobilized within hours. Palo Alto Networks' Unit 42 **tracked 149 DDoS attacks across 16 countries within 72 hours,and over 600 cyberattack claims across 100+ Telegram channels.** Iranian APT groups with established European infrastructure, including APT34, MuddyWater and APT42, have intensified operations.

Command-and-control traffic routed through fabricated European companies, phishing kits intercepting MFA tokens in real time and pre-positioned infrastructure activated on short notice. These are documented, active operations.

Russian cyber and hybrid activity against European NATO members remains persistent. Pro-Russian hacktivist group NoName057(16) **claimed 4,693 attacks in 2025** and pro-Russian and pro-Iranian hacktivist ecosystems formally c**onverged in early March 2026**. **Ransomware, meanwhile, jumped 45-58% in 2025 with over two-thirds of attacks hitting businesses under 500 employees.**

CrowdStrike's 2026 report records **average breakout times of 29 minutes, with 82% of detections malware-free**, meaning traditional signature-based tools cannot see them.

149
DDoS attacks

in 16 countries
within 72 hours

45 - 58%
ransomware in 2025

2/3 of attacks on
businesses < 500 employees

29 minutes
avg. breakout record

with 82% of detections
malware-free

SECTION 5
The workforce gap that hiring cannot close

Europe has roughly **1.4 million cybersecurity professionals** and **needs 1.8 million**. A **400,000-person shortfall**, per ENISA, that is getting worse, not better.
The continent's cyber workforce actually **contracted by 0.7% in 2024.** Germany alone faces a **projected shortage of 106,000 workers by 2026**.

400.000
cyber professionals shortfall in Europe

106.000
cyber professionals shortage in Germany

But the more important finding from ISC2's 2025 study is this: for the first time, 52% of cybersecurity leaders said the real issue is not having the right skills, rather than not having enough people. **Critical skills shortages affect 59% of teams.**
Nearly half of all professionals say they feel exhausted trying to stay current. This is a problem that hiring alone cannot solve, because the **people with the right skills are already employed and already burning out.**

This is precisely why the **agentic augmentation model matters.** Not as a replacement for skilled professionals, but as the **only realistic way to bridge the gap** between what teams can handle and what the threat landscape demands.

A two-person security team running CYBERQUEST and NETALERT gets investigative throughput that would traditionally require six to eight analysts across multiple tools. **Not because the platform replaces analysts, but because it eliminates the manual, repetitive correlation work that consumes 70% of their day. The analyst focuses on judgment, context and decision-making.** The platform handles volume, correlation and enrichment. That division of labour does not just improve security outcomes. **It makes the job sustainable.** And in a market where burnout is hollowing out teams faster than universities can produce graduates, sustainability matters.

> "Nextgen Software is not selling a replacement for your security team. It is selling the thing that might actually keep your security team from walking out the door."

The window is open

Everything in this document points in the same direction. Threats are intensifying and will not ease. Regulation is tightening and will not relent. The workforce gap is structural and will not close through hiring alone. Economic headwinds are making every investment decision harder. And the US vendor ecosystem, for all its capability, is priced for a market that most European organisations do not belong to.

CYBERQUEST and NETALERT from Nextgen Software offer a different path. European-built, European-hosted.

- A **consolidated SIEM and NDR platform with agentic investigation capabilities** that give small teams the analytical reach of departments three times their size.
- Detection logic engineered for the **European threat landscape**.
- **Compliance coverage mapped to NIS2, DORA and GDPR** with auditable evidence built in.
- Deployed in days.
- **Priced for European business realities.**

The organizations that act with clarity and pragmatism will come through this period stronger. The ones that delay will carry risk they did not need to carry.

To explore how CYBERQUEST and NETALERT can work for your organisation, visit nextgensoftware.eu

nextgen

CQ CYBERQUEST

NETALERT

Questions? Contact us.

www.nextgensoftware.eu
office@nextgensoftware.eu
marketing@nextgensoftware.eu