The Atomic Bomb We Haven't Faced (Yet): Inside Cybersec Europe and the Future of Cybersecurity

Entering the expo in Brussels, the scale was immediately apparent, both in the sheer number of people (193 exhibitors and thousands of IT professionals) and in the weight of the challenges they had come to address. The tone was set by the opening speaker: Eléonore Simonet, Belgium's Minister of Small and Medium Enterprises (SMEs), who at 27 is the youngest minister ever appointed to a Belgian federal government. Her message was direct: Hackers don't care how small your business is. This problem requires expertise and investments, both of which smaller businesses cannot spare, which is why both the European Union and the Belgian government are working to make cybersecurity guidelines more accessible and industry-specific.

Mythos

Senior Vice President for Cybersecurity at NTT Data, Stefaan Hinderyckx, called it the atomic bomb of cybersecurity: Mythos. Anthropic's new model is an industry-first AI that is capable of autonomously finding, assessing, exploiting and "capturing the flag" in a target system, without human intervention. To understand what that means: in cybersecurity, capturing the flag is the benchmark for fully compromising a system. Average breakout times have fallen to 29 minutes, with the fastest observed just 27 seconds, and Mythos may compress this further. According to the UK's AI Security Institute (AISI), Mythos succeeds at expert-level tasks 73% of the time in controlled environments without active defenders. At a compute cost of up to 100 million tokens, it completed a simulated 32-step corporate network takeover in 3 out of 10 attempts, which would take a human expert around 20 hours. Worth noting is that these tests were conducted in weakly defended systems, with no active incident response. It is an important question to ask whether Mythos would perform at the same level against a well-defended organisation.

There are however concrete measures that businesses can take to protect themselves. Across the expo floor, companies demonstrated their defensive architectures. Three measures stood

out consistently: First, zero-trust architecture: continuous verification for every device and user. No implicit trust is granted to anyone both inside and outside the network.
Second, technology consolidation: Reducing a fragmented tool stack for fewer, but with better integrated systems that enforce consistent policy and cleaner telemetry. As Hinderyckx put it, this is as much an economics argument as a security one.
Third, AI-powered endpoint protection: A ransomware protection company showed me that AI agents deployed on endpoints can monitor activity in real time, allowing them to intercept encryption keys mid-attack, before ransomware lock completes, at machine speed.
A final measure, less glamorous but no less critical: Multifactor Authentication (MFA). Its absence is one of the most exploited vulnerabilities across organisations.

While speaking to the small and medium cybersecurity firms, their opinion was cooler and less impressed by the AI hype. Their argument: AI is a powerful tool, but it remains a tool that cannot be trusted without a human who fully understands its output and knows how to correct it, particularly on the defensive side. Offensive AI often produces false positives, flagging vulnerabilities that are not exploitable. Therefore, they argue that the exploitation window is still small, and Mythos's impact is contested.

Both positions point to the same conclusion: AI has already lowered the floor of offensive capability. Whether or not Mythos raises the ceiling to existential levels, its trajectory is steep.

NIS2: Good governance, troubled enforcement

In a digital world of expanding vulnerabilities, the old mentality no longer holds. For decades, cybersecurity was treated as an IT concern, and Operational Technology (OT), systems running factory floors, energy grids and hospitals, were considered separate from the digital threat landscape entirely. This assumption is antiquated, which is what the European Union aims to solve with its NIS2 regulation package. To the relief of many cybersecurity experts, CEOs of companies are now personally held responsible for the cybersecurity posture of their organisations, forcing them to report incidents up the chain to ENISA. Furthermore, NIS2 extends to OT systems in critical sectors. If a hacker manages to shut down hospital equipment or factory safety systems, it would not be just an IT problem, but a crisis.

For SMEs, the EU is currently building tailored, industry-specific guidelines, while the Cyber Resilience Act (CRA) extends mandatory requirements to connected products that are sold in the EU. Efforts such as these show rule makers understand what European companies need, which is a change in cybersecurity mentality.

Asking multiple experts the same question: “Where do you see the gap between NIS2 and what is actually needed?”, produced a strikingly consistent answer: there is a need for an EU-level enforcement body, and genuine homogenisation of the implementation of the rules across member states. NIS2 is already the minimum baseline of cybersecurity, but across the EU, member states are applying it unevenly, without consistent enforcement. The weakest link becomes everyone’s liability. The call is in this case not for new rules, but for the existing ones to bite. Possibly through an EU-level body that would be strictly enforcing companies to conform to NIS2.

To conclude, whether Mythos proves to be cybersecurity's atomic bomb or a tool defenders learn to absorb, the open question Cybersec left is: how hard will it hit? What the conference made clear is that Europe is building its shelters with regulation, architecture, and collective awareness. NIS2 brings cybersecurity to the corporate boardroom, and the CRA bakes it into products. Enforcement remains the critical gap in the regulation, but the direction is right.

The most important change is cultural. The head of the cybersecurity unit at the Council of the European Union, Liliana Mușețan, describes resilience as an ethos that you have to share. From the SME owner who assumes that they are too small to be a target, to the employee who opens a phishing link, to the CEO who has pushed the responsibility to the IT department, to the member state that applies NIS2 selectively, the weakest link is always human.