New Titania Whitepaper Warns: AI Is Turning Flat Networks Into Fast Failures

As DORA and NIS2 enforcement ramps up, financial institutions are under pressure to prove segmentation and resilience or face serious consequences.

ARLINGTON, VA, UNITED STATES, August 27, 2025 /EINPresswire.com/ -- Titania, the award-winning cybersecurity automation software company, today released a new whitepaper warning that flat, unsegmented networks are becoming a critical liability for European financial institutions. As enforcement of DORA (Digital Operational Resilience Act) and NIS2 directives intensifies, institutions are being asked to do more than show policy; they must prove operational resilience.

Complicating that challenge is the rise of AI-driven ransomware. According to Gartner, AI agents will reduce the time it takes to exploit exposed accounts by 50% by 20271. That's reshaping ransomware from a creeping threat into a real-time crisis. In 2024 alone, ransomware was linked to one-third of all breaches. Meanwhile, nearly 40% of financial firms still can't demonstrate full compliance with DORA or NIS2.

The new whitepaper titled "Reclaiming Control: How Financial Services Can Pre-empt, Prevent and Contain Ransomware with Network Segmentation" outlines how macro segmentation can dramatically reduce exposure and protect core assets, even as threats evolve.

"The combination of AI-powered attacks and live compliance enforcement has made flat networks a liability," said Phil Lewis, Senior Vice President of Market Strategy and Development at Titania. "Network segmentation assurance is no longer optional — it's foundational to operational resilience and regulatory readiness."

"DORA and NIS2 are pushing financial firms to adopt architectures that can contain and withstand modern attacks — and segmentation is central to that," said Jim Seaman, Director and Senior Security Consultant at IS Centurion Consulting. "We know organizations are still struggling with implementing segmentation practices - so we've put together a free guide to help with this.

Titania's whitepaper includes practical recommendations for aligning technical policies to evolving regulatory requirements and introduces a framework for assuring that segmentation is maintained after every change.

The guide also covers how to assure that the network remains segmented after every change. Seaman continues “Organizations need to acknowledge that their networks change daily, and every unchecked change is a risk that ransomware could exploit.”

Key topics covered in the guide include:

· How AI is accelerating ransomware attacks and compressing response windows

· Why flat networks pose a critical risk under DORA and NIS2 regulations

· The role of macro- and micro-segmentation in reducing ransomware impact

· Why continuous validation of segmentation is essential for resilience

· How financial institutions can align with DORA and NIS2 to avoid disruption and penalties

With potential penalties under DORA reaching up to 2% of global annual turnover, the cost of inaction is high. Titania’s new guide provides actionable steps for security leaders looking to future-proof their network architectures against both regulatory scrutiny and real-world threats.

Download the full whitepaper here.

Florie Lhuillier
CCGroup Communication
titania@ccgrouppr.com
