Swiss Papers AG Launches Obsidio for Realistic DDoS Resilience Testing

Innovative Swiss security technology against global cyber threats. Papers AG launches "Obsidio" for highly realistic DDoS resilience testing

Alessandro De Carli, CEO Papers AG, Switzerland

ZUG, SWITZERLAND, June 5, 2026 /EINPresswire.com/ -- Innovative Swiss security technology against global cyber threats:
Papers AG launches "Obsidio" for highly realistic DDoS resilience testing

Against the backdrop of growing global cyber threats and the increasing vulnerability of critical digital infrastructure, the Switzerland-based software company Papers AG is introducing Obsidio, a security solution that is unique in its kind, to the market. Already in use by renowned banks, the solution enables financial institutions and operators of critical infrastructure to proactively, realistically, and continuously put their resilience to cyberattacks through its paces, rather than reacting only in an emergency. The new application is specifically designed to meet the documentation requirements mandated by Swiss and European regulatory authorities.

Proactive Protection in Times of Drastically Increasing Cyber Attacks
Conventional security tests often reach their limits because they merely simulate attacks in artificial laboratory environments. Obsidio, on the other hand, uses a globally distributed infrastructure of currently over 232,000 smartphones to precisely replicate realistic distributed denial-of-service (DDoS) attacks. In a DDoS attack, a system is crippled by a massive number of simultaneous requests—comparable to thousands of people simultaneously blocking the entrance to a building.*

Digital Sovereignty and “Swissness” as Core Principles

Especially for Switzerland, whose security can be viewed less and less in isolation from the international technology and cyber risk landscape, Obsidio creates a practical approach to strengthening the digital resilience of critical systems. As a renowned tech powerhouse based in Zug, Papers AG relies on Swiss engineering expertise and the highest data protection standards:

- Decentralized security: By utilizing the Acurast platform developed by Papers AG, which distributes computing power across tens of thousands of real-world devices
- worldwide, Obsidio avoids dependence on large, centralized cloud providers and reduces systemic risks.
- NSA immunity: Thanks to processing in secure hardware areas of mobile devices, the infrastructure is structurally protected against unauthorized external access and extraterritorial control.
- Data protection: The system operates according to strict zero-trust principles, is fully GDPR-compliant, and protects the privacy of all participating users through their explicit consent (opt-in).

> Obsidio transforms cyber resilience management from reactive damage control to proactive verification of defense systems.”
>
> *Alessandro De Carli, CEO Papers AG*

Compliance with regulatory requirements (FINMA & DORA)

For Banks and insurance companies, demonstrating operational resilience is now a regulatory necessity. Obsidio provides cryptographically signed and tamper-proof logs that serve as evidence for audits. By providing meaningful test results, the platform delivers central evidence of operational resilience specifically designed to meet the reporting requirements under FINMA (Swiss Financial Market Supervisory Authority), DORA (EU Digital Operational Resilience Act), and NIS2 (EU Network and Information Security Directive 2).

“At a time when trust in digital tools is the greatest asset, Obsidio offers a unique platform that underpins this trust through measurable resilience,” says Alessandro De Carli, CEO of Papers AG. “Obsidio transforms cyber resilience management from reactive damage control to proactive verification of defense systems.”

---

*Background: What is a DDoS attack? A DDoS (Distributed Denial of Service) attack is a cyberattack in which a large number of devices or servers simultaneously send artificial requests to a website, platform, or digital infrastructure. The goal is to overload the system so that it becomes slow, crashes, or becomes completely inaccessible to legitimate users. For banks, government agencies, telecommunications providers, hospitals, or other critical infrastructure, such attacks can cause significant operational, financial, and reputational damage.

Global DDoS attacks have evolved from minor digital disruptions into powerful economic and geopolitical weapons that target critical infrastructure. They inflict massive financial and reputational damage on businesses worldwide through forced downtime and ransom extortion. Today, state-sponsored actors and hacktivists frequently deploy these attacks as a primary tool of cyber warfare during international conflicts. Driven by AI and compromised cloud networks, modern attacks have reached unprecedented, hyper-volumetric scales that traditional defenses cannot handle. Consequently, robust DDoS mitigation has become a baseline survival requirement for modern organizations and governments.

About Obsidio
Obsidio is a "Swiss-engineered resilience testing platform" developed specifically for critical infrastructure. The platform enables realistic, decentralized simulations that accurately reflect the dynamics of real cyberattacks. Against the backdrop of growing global cyber threats and the increasing vulnerability of critical digital infrastructure, Obsidio offers organizations the opportunity to test their resilience not only in an emergency, but in a controlled, realistic, and proactive manner. The application, developed by Zug-based Papers AG, ensures maximum reliability for critical communication environments and is frequently used by leading financial institutions.

Obsidio exclusively offers advanced DDoS (Distributed Denial of Service) resilience solutions that enable organizations to transition from reactive damage control to proactive vulnerability management. By integrating the decentralized cloud computing protocol Acurast, Obsidio is redefining the standards for security and censorship resistance. Acurast addresses the core problem of centralization, inefficiency, and fragility in traditional cloud computing infrastructures, which require massive capital expenditures. The protocol transforms unused or discarded smartphones into a global, decentralized mesh cloud of verifiable and trusted compute providers. By simulating a realistic botnet, Obsidio can uncover vulnerabilities—something that would not be possible with the centralized providers available on the market. Obsidio uses this botnet, sourced from ethically sound providers, to carry out realistic attacks. By being based in Zug, Obsidio leverages the regulatory clarity and technological excellence of Switzerland’s leading technology hub. The infrastructure follows strict zero-trust principles and, thanks to decentralization, is completely independent of large, centralized cloud providers. By precisely simulating such attacks using a realistic botnet, vulnerabilities can be uncovered that could not be detected using centralized providers available on the market.

Peter Zimmermann
Huber & Partner PR AG / Press Contact
+41 44 385 99 99
email us here
Visit us on social media:
LinkedIn