Resilient. Bewiesen.

Obsidio

Testen sie ihre Abwehr mit realen DDoS Simulationen.
Swiss Made.

Regulatorische Anforderungen

Resilienz ist geschäftskritisch. Nachweise sind Pflicht.

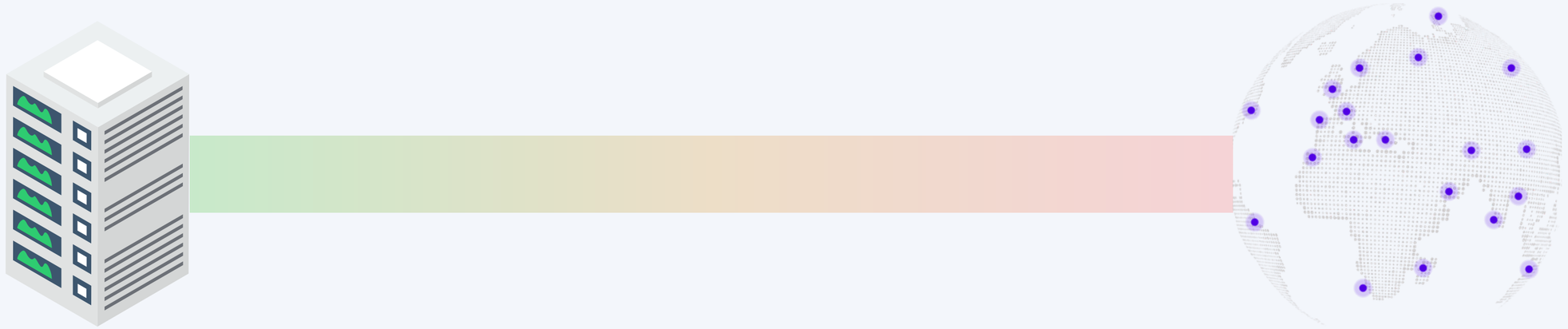
Aufsichtsbehörden fordern von Unternehmen den Nachweis von Cyber-Resilienz. Beispiele: FINMA Zirkular 2023/1 für Finanzakteure. DORA für europaweit tätige Unternehmen.

Institutionen müssen belegen, dass ihre Infrastruktur gegen DDoS Attacken geschützt ist und regelmässig getestet wird.

Non-Compliance bedeutet: Ausfallzeiten, Reputationsschäden und Vertrauensverlust, bei Kunden wie Vorständen.

Kontext

Bedrohungen sind dezentral. Herkömmliche Tests nicht.



Heutige Testlösungen sind zentralisiert, Simulationen kommen aus wenigen Rechenzentren.

Moderne Cyberbedrohungen kommen aus globalen, dezentralen Botnets Tausender verteilter Geräte.

Das Ergebnis: Simulationen bilden reale Angriffsmuster nicht ab.
Organisationen bleiben unvorbereitet.

Obsidio

Resilienz-Tests im Self-Service

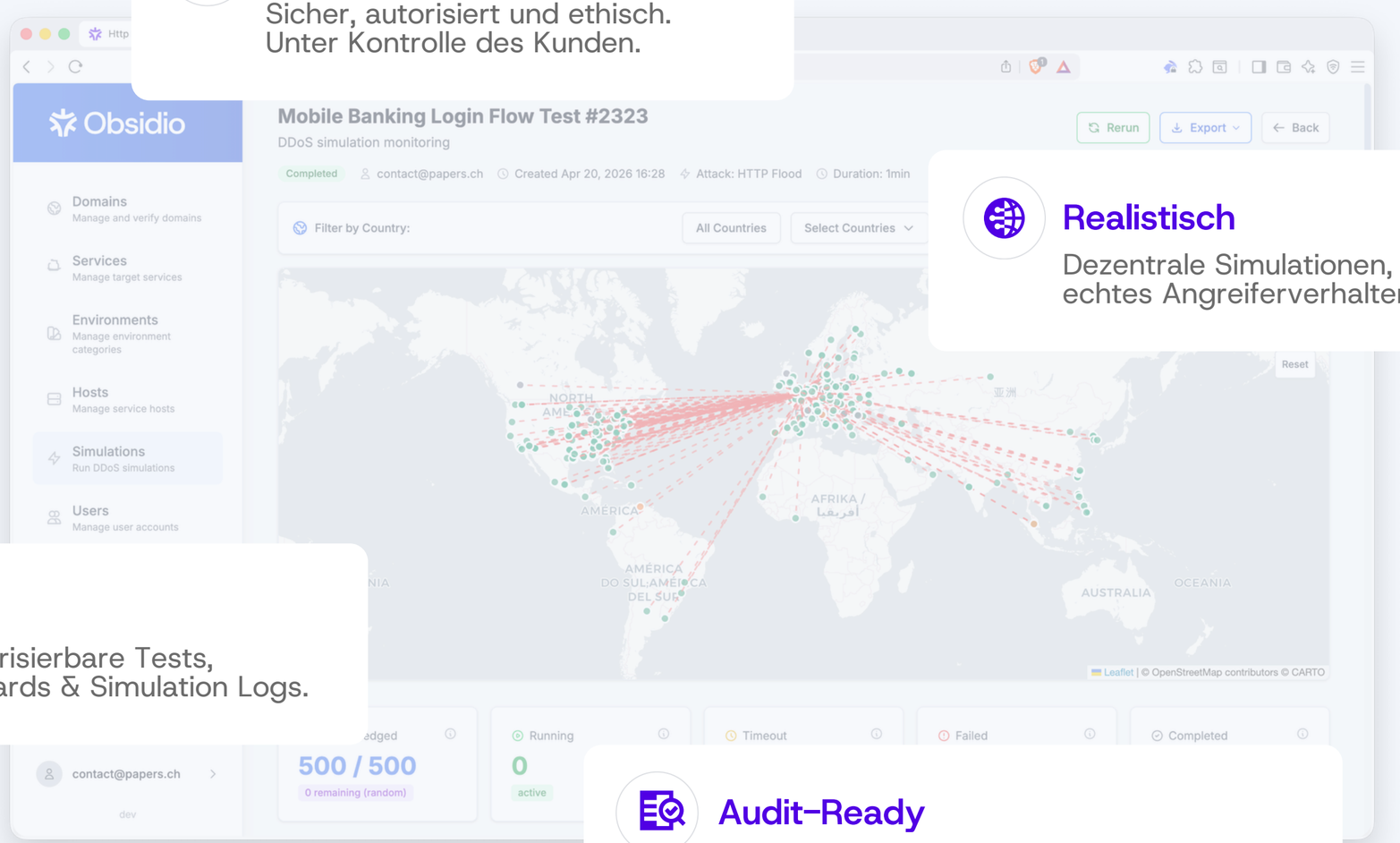
Wie Obsidio aus Anforderungen belastbare Ergebnisse macht.

Produktübersicht

Entwickelt für CISOs, CROs und Security-Teams.

Kontrolliert

Sicher, autorisiert und ethisch.
Unter Kontrolle des Kunden.



Realistisch

Dezentrale Simulationen,
echtes Angreiferverhalten.

Self-Service

Individuell parametrisierbare Tests,
skalierbar, Dashboards & Simulation Logs.

Audit-Ready

Auditgerechte Reports für Regulatoren,
Vorstände und Compliance-Teams.

So funktioniert's

Gewissheit in vier Schritten.

Authorisierung

Eigentümerschaft per DNS verifizieren. Manipulationssicher.

Konfiguration

Simulationstyp, Umfang und Dauer festlegen.

Simulation

Dezentrale Tests in kontrollierter Umgebung durchführen.

Reporting

Belastbare, auditierbare Nachweise erhalten.

Differenzierung

Synthetische Tests vs. belastbare Resilienz.

Bisher	Mit Obsidio
Last aus Rechenzentren → Synthetischer Traffic	40K+ aktive Geräte weltweit → Realistische Simulationen
Mässiger Realismus → Angriffe sind einfach zu blocken	Echte Netzwerk-Topologie → Echte Angriffsdynamiken
Fragmentierte Berichte → Kaum auditkonform	Auditfähige Ergebnisse → Konzipiert für Regulatoren
Komplexer Betrieb → Viel Setup, externe Teams	Self-Service → Leicht bedienbar, autonome Teams
Auch dubiose Darknet-Anbieter → Compliance Risiko	Ethisch beschaffte Geräte → Verifiziert, sicher & compliant

Technologie

Tausende echte Geräte. Ethisch beschafft.

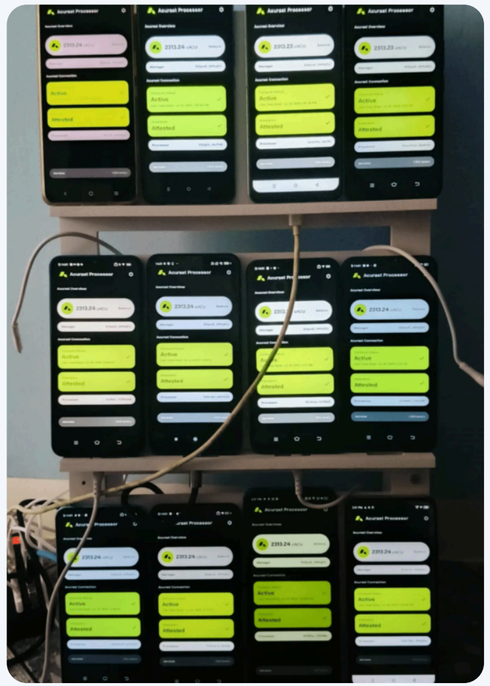
- Obsidio nutzt 40'000+ aktive Geräte von Acurast. Wie ein echtes, sicheres Botnet.
- Geräte an privaten Internetanschlüssen. In über 175 Ländern.
- Simulationen laufen ausschliesslich in Trusted Execution Environments (TEEs).
- Attestiert, verifizierbar, vertraulich. Sicherheit auf Enterprise-Level.

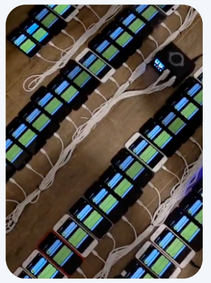
Über Acurast
www.acurast.com

Sparring Partner

Ihr Gegner.
Echte Geräte. Echter Traffic. Echte Angriffe.

Echte Device-Fingerprints. Global verteilt. 24/7 bereit.





Fallstudie

Wie eine führende Schweizer Bank mit Obsidio ihre Resilienz nachweist.

Story

Eine der fünf größten Schweizer Banken musste ihre Resilienz gemäß FINMA-Zirkular 2023/1 validieren.

Bisherige Optionen waren veraltete, zentralisierte Tests oder unregulierte Anbieter aus der Grauzone. Mit entsprechenden Compliance-Risiken.

Mit Obsidio führt die Bank heute regelmässig realistische, dezentrale Simulationen durch: kontrolliert, ethisch einwandfrei und mit auditfähigen Reports für Regulatoren und Vorstände.

Outcome

Von synthetisch zu **realistisch**: Simulationen bilden echte Angriffsdynamiken ab.

Von sporadisch zu **regelmässig**: DDoS Testing ist nun ein integraler Prozessschritt, um die Abwehr zu härten.

Von riskant zu **konform**: Kein Grauzonen-Testing, FINMA-konform.

Von unklar zu **auditfähig**: Messbare Nachweise, denen Regulatoren und interne Governance vertrauen.

Obsidio

Swiss Made.
Fundierte Expertise.

Diskret. Bewährt bei führenden Institutionen.

Business Model

Flexibel für jede Organisation.

Credit System

Nur zahlen, was genutzt wird. Abrechnung nach Bot User Minutes.
Volle Flexibilität und Transparenz.

Enterprise Agreements

Verträge auf Monats- oder Jahresbasis.
Für planbares, kontinuierliches Testing.

Individuelle Nutzung

Skaliert nach Kunde.
Von Einzeltests bis zu kontinuierlichen Programmen.

Jetzt starten

Erst testen, dann selbst loslegen.

Proof Of Value

Testkonto erhalten.

Testumfang definieren.

4 Wochen voller Self-Service-Zugang.

Praxisnahe Evaluation.

Voller Support und Training.

Einmalige, anrechenbare Gebühr.

Procurement

Individuelle Vereinbarung erarbeiten.

Vertrag aufsetzen.

Formale Anbieterfreigabe, falls erforderlich.

Finale Plattform einrichten.

Individuelle Anpassungen spezifizieren und erhalten.

Self-Service

Benutzer eigenständig verwalten.

Zielumgebungen managen.

Tests durchführen, Reports erstellen, Daten exportieren.

Guthaben aufladen.

Support, Training und Beratung nach Bedarf.

Resilienz beweisen.

Obsidio

Regulatorische Anforderungen souverän erfüllen.

Sprechen Sie mit Experten

Verlangen sie eine Demo

Obsidio
Papers AG
Baarerstrasse 43
6300 Zug
Schweiz

+41 44 512 90 04
hi@obsidio.com
www.obsidio.com

Oder sprechen sie mit unserem Vertriebspartner:

emitec
datacom