Verein für Technische
& Digitale Resilienz
(VTDR) i. G.

KRITIS 3.0 – Das passive Frühwarnsystem für moderne digitale Resilienz

KRITIS 3.0 ist ein neuartiges Frühwarnsystem, das die externe Sicherheitslage digitaler Dienste ganzheitlich bewertet. Es analysiert technische Schwachstellen, regulatorische Anforderungen und inhaltliche Manipulationen allein anhand öffentlich sichtbarer Daten – vollständig passiv, ohne Scans, ohne Zugangsdaten und ohne Eingriff in produktive Systeme.
Damit schließt KRITIS 3.0 genau jene Sicherheitslücke, die Angreifer systematisch ausnutzen: den Blick **auf das System von außen**.

Die Plattform kombiniert drei Analysebereiche zu einem integrierten Sicherheitsmodell:

1. Passive technische Analyse

KRITIS 3.0 erkennt Schwachstellen, unsichere Header, veraltete Komponenten, exponierte APIs, verwundbare Bibliotheken und fehlerhafte Konfigurationen allein durch die Auswertung externer Informationen. Die Analyse folgt etablierten Standards wie **BSI-IT-Grundschutz**, **ISO 27001**, **OWASP** und macht Risiken sichtbar, die interne Sicherheitssysteme oft übersehen.

2. Automatische Compliance- und Härtungsbewertung

Alle technischen Findings werden automatisch den Anforderungen aus **NIS-2**, **ISO 27001** und **BSI** zugeordnet. Daraus entstehen **prüffähige Audit-Nachweise** und nachvollziehbare Härtungsempfehlungen, die sofort in Sicherheitsprozesse integriert werden können. Dadurch reduziert KRITIS 3.0 den Aufwand für Zertifizierungen und verbessert die Nachweisführung gegenüber Aufsichtsbehörden erheblich.

3. KI-basierte Inhaltsintegrität (Implementierung Q2-2026)

KRITIS 3.0 überwacht nicht nur die Infrastruktur, sondern auch die **tatsächlich ausgelieferten Webinhalte**. KRITIS 3.0 erkennt:

- verdeckte Link-Manipulationen und unerwünschte SEO-Spam-Einträge (z. B. automatisch eingeschleuste Verweise auf externe Pharma-, Glücksspiel- oder Werbedomains),
- unautorisierte Skript-Einbindungen,

- defacement und strukturelle Änderungen an Texten, Medien oder Layouts,
- kurzfristige, automatisiert eingefügte Schadcode-Elemente, die von klassischen Scannern nicht erfasst werden.

Diese Form der Inhaltsüberwachung ist bislang in keiner anderen Sicherheitslösung integriert – weder in klassischen Scannern, noch in WAFs, noch in Monitoring-Systemen.

KRITIS 3.0 liefert **frühzeitige, präzise Risikoerkenntnisse**, stellt automatisch **auditfähige Compliance-Nachweise** bereit und schützt zuverlässig vor unbemerkten Manipulationen und externen Eingriffen.

Die Plattform ist als **skalierbare SaaS-Lösung** konzipiert und deckt einen stark wachsenden europäischen Markt ab, der insbesondere durch **NIS-2**, gestiegene Anforderungen an Websicherheit und zunehmende Angriffsfrequenzen getrieben wird.
Durch den wissenschaftlich fundierten, vollständig passiven und datenschutzfreundlichen Ansatz stärkt KRITIS 3.0 messbar die **digitale Resilienz und Souveränität** moderner Organisationen – gerade dort, wo technische Sicherheit, regulatorische Anforderungen und der Schutz digitaler Inhalte zugleich relevant sind.

Ronny Woick
Information Security Officer (certified) & IT-Berater
Verein für Technische & Digitale Resilienz (VTDR) i. G.

✉ **E-Mail: r.woick@vtdr.de**
🌐 **Web: https://vtdr.de/**
📞 **Telefon: +49 176 829 63 295**