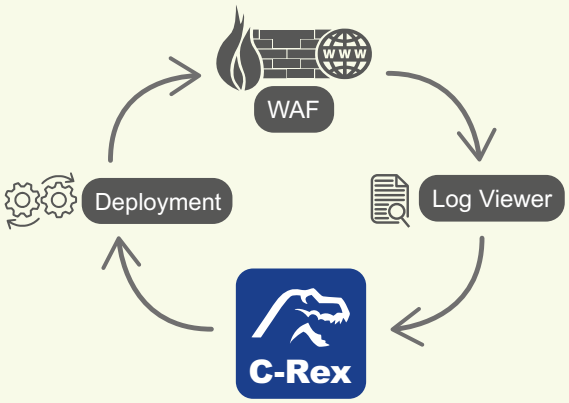
# C-Rex by netnea
# für eine starke WAF

**C-Rex ist eine Tool-Suite zum automatisierten und intuitiven Handling der False Positive Alarme von Web Application Firewalls (WAF). C-Rex unterstützt alle WAFs, die auf ModSecurity bzw. OWASP CRS basieren.**




## ? Die Aufgabenstellung

ModSecurity basierende WAFs sind ein extrem wirksames Instrument gegen Angriffe auf Webanwendungen ...

… wären da die nicht die Fehlalarme. Denn je restriktiver und damit wirksamer eine WAF konfiguriert ist, desto größer die Anzahl der Fehlalarme.

Sie arbeiten in einem Unternehmen der Finanzindustrie und unterliegen dem Payment Card Industry Data Security Standard? Web Application Firewalls zu C-Rex finden Sie hier: https://c-rex.netnea.com/downloads/c-rex-pci.pdf

## ! Die Lösung
## einfach – zuverlässig – sicher – günstig

C-Rex erkennt bis zu 99 Prozent aller Fehlalarme automatisiert und unterstützt bei deren Behandlung. Sicher, intuitiv und effizient. Ihre scharf geschaltete WAF schützt Ihre Webapplikationen optimal; C-Rex kümmert sich um die Fehlalarme und fügt sich in das DevOp Setup ein.

## X Gängige Unternehmenspraxis heute
## umständlich – unzuverlässig – unsicher – teuer

### Manuelle Behandlung der Fehlalarme

Viele große Unternehmen mit kritischen Webanwendungen beschäftigen heute Mitarbeiter oder ganze Teams, die Fehlalarme sichten, klassifizieren und behandeln. Denn das SOC ist weit weg von der Applikation und tut sich schwer die Alarme korrekt zu klassifizieren. Der Nachteil: Der Prozess ist aufwändig, langsam und teuer – egal wie Unternehmen ihn organisieren.

### Entschärfen der WAF

Je weniger restriktiv die WAF ist, desto weniger Fehlalarme. So lösen manche Unternehmen das Problem, indem sie ihre WAF entschärfen. Der Nachteil: Sie werden anfällig für Angriffe.

### WAF im Detection Only Modus

Viele Unternehmen schalten ihre WAF gar nicht erst scharf. Der Nachteil: Trotz teurem WAF-Betrieb sind die Webanwendungen ungesichert.

C-Rex

# 5 gute Gründe
# für den Einsatz von C-Rex

**1.**

## Messerscharf …

**… identifiziert C-Rex die Fehlalarme aus den Log-Dateien.**
Bereits direkt nach der Installation erkennt C-Rex bis zu 90 Prozent der Fehlalarme. Nach der Optimierung sind es bis zu 99 Prozent. Und: Je länger C-Rex im Einsatz ist, desto besser wird die Erkennungsrate. Unternehmen können ihre WAF scharf schalten und ihre Anwendungen schützen, denn Fehlalarme behindern nicht länger den Betrieb.

**2.**

## Einfach und intuitiv …

**… können Entwickler Fehlalarme selbst behandeln.**
Die C-Rex Automatisierungen und das GUI machen den Betrieb ganz ohne ModSecurity Spezialwissen möglich. Denn C-Rex bringt das gesamte Know-how mit. Es assistiert nicht nur, sondern schlägt Regelmodifikationen vor, die das Team nur noch ausrollt.

**3.**

## Know-how und Erfahrung …

**… aus 20 Jahren haben wir in C-Rex investiert.**
Entwickler Dr. Christian Folini ist nicht nur ein erfahrener Cybersecurity Consultant. Er ist auch Autor des ModSecurity Handbuchs und an der Entwicklung des OWASP CRS beteiligt. Christian organisiert übrigens auch den Support und schlaut Ihre Mitarbeiter auf (siehe Grund 5). Vereinbaren Sie einen Termin mit Christian Folini.

**4.**

## Weiterarbeiten wie gewohnt …

**… im DevOps Setup, das sich bewährt hat.**
Denn C-Rex fügt sich in die bestehenden Architekturen und Prozesse ein, ohne eine Veränderung nötig zu machen. C-Rex verarbeitet die existierenden Log-Dateien, kreiert einen HTML-Report und schlägt Rule Exclusions vor. Deren Implementierung erfolgt unabhängig von C-Rex über die existierenden Infrastrukturen und Prozesse. Der Betrieb erfolgt auf der Kundeninfrastruktur in der Cloud oder on-premise. Sämtliche Daten, die C-Rex verarbeitet, verbleiben ausschließlich in der Infrastruktur unserer Kunden.

**5.**

## Lieber alles selber machen …

**… und eigenes Know-how aufbauen.**
Mit ModSecurity, CRS und C-Rex behalten Unternehmen die volle Kontrolle und machen sich nicht von kommerziellen Anbietern abhängig (Stichwort „Digitale Souveränität“). Wir teilen unser Wissen und unsere Erfahrung gerne. Denn ModSecurity Experten sind gefragt und schwer zu finden. Mit unseren Schulungen versetzen wir die Mitarbeiter unserer Kunden in die Lage, das Thema WAF selbst zu betreiben – vom Aufsetzen der WAF bis zum täglichen Betrieb mit C-Rex.

Sie arbeiten in einem Unternehmen der Finanzindustrie und unterliegen dem Payment Card Industry Data Security Standard? Web Application Firewalls zu C-Rex finden Sie hier:
https://www.pcisecuritystandards.org/standards/pci-dss/

C-Rex

# C-Rex by netnea
# Ihre Ansprechpartner

## Über netnea

netnea ist ein spezialisiertes Schweizer IT-Unternehmen mit Schwerpunkt auf Cybersicherheit und Netzwerk Monitoring. Als anerkannte Experten im Bereich Open-Source-Sicherheitslösungen hat netnea über 25 Jahre Erfahrung bei der Unterstützung von sicherheitssensiblen Unternehmen und Institutionen. netnea ist führend im Bereich WAF-Integration, Tuning von False Positives und der Schulung von Mitarbeitenden auf diesen Themen. Das Unternehmen steht für digitale Sicherheit auf höchstem Niveau.

## Der Experte – Christian Folini

**Zur Person:**
LinkedIn Profil

Weil ihm False Positives schon immer ein Dorn im Auge waren, hat Dr. Christian Folini C-Rex entwickelt. Der Security Engineer ist Partner bei netnea. Er leitete mehrere Jahre das OWASP CRS Projekt. In seinen Schulungen vermittelt er das Know-how, um ModSecurity und CRS skalierend zu betreiben. Christian wurde als „OWASP Distinguished Lifetime Member“ ausgezeichnet.

## Ihr Ansprechpartner – Alexander Glatzeder

**Jetzt Termin vereinbaren**

**Zur Person:**
LinkedIn Profil

Alexander Glatzeder, mit Sitz in Neuchatel in der Schweiz, ist seit mehr als zwanzig Jahren in der IT-Branche aktiv, seit 2015 als Director Sales bei freyraum marketing. Als Vertriebspartner unterstützt freyraum marketing netnea und deren Kunden bei Information, Beratung und Lizensierung von C-Rex.

**Telefon:**
+49 176 24471851

**E-Mail:**
alexander.glatzeder@freyraum-marketing.de

**Mehr Informationen zu C-Rex finden Sie hier:**
https://c-rex.netnea.com/

C-Rex