Kiteworks

COMPLIANCE-INFORMATION

# Erfüllung der Anforderungen des Cyber Resilience Act der EU

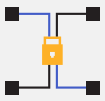
## Für Produkte mit digitalen Elementen bietet Kiteworks ein umfassendes Sicherheitsmanagement

Der Cyber Resilience Act (CRA) führt Cybersicherheitsanforderungen für Produkte mit digitalen Elementen auf dem EU-Markt ein. Ziel ist es, die Sicherheit von Hard- und Softwareprodukten während ihres gesamten Lebenszyklus zu verbessern und es den Nutzern zu ermöglichen, die Cybersicherheit bei der Auswahl und Nutzung digitaler Produkte zu berücksichtigen. Zu den wichtigsten Bestimmungen gehören grundlegende Cybersicherheitsanforderungen für Hersteller in Bezug auf Produktdesign, Entwicklung und Schwachstellenmanagement, Verfahren zur Konformitätsprüfung einschließlich der Bewertung kritischer Produkte durch externe Parteien, Transparenzverpflichtungen in Bezug auf Sicherheitsmerkmale und Aktualisierungen sowie Marktüberwachungs- und Durchsetzungsmechanismen. Das Gesetz gilt bis auf wenige Ausnahmen für alle vernetzbaren Hard- und Softwareprodukte. Die Nichteinhaltung des EU-Cyber Resilience Act kann zu empfindlichen Geldstrafen von bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes führen, je nachdem, welcher Betrag höher ist. Zusätzlich zu den finanziellen Folgen können Unternehmen, die die Vorschriften nicht einhalten, mit Marktzugangsbeschränkungen, Rufschädigung und verstärkter behördlicher Kontrolle konfrontiert werden, was zu erheblichen Beeinträchtigungen der Geschäftstätigkeit und zum Verlust von Wettbewerbsvorteilen auf dem EU-Markt führen kann. Ziel der Richtlinie ist es, einen kohärenten EU-Rahmen zu schaffen und eine Fragmentierung der nationalen Regelungen zu vermeiden, während gleichzeitig die Sicherheit und das Vertrauen der Nutzer in digitale Produkte gestärkt werden.

### Bewertung und Management von Cybersicherheitsrisiken mit einer Secure-by-Design-Plattform

Der CRA verlangt eine umfassende Bewertung der Cybersicherheitsrisiken für Produkte mit digitalen Elementen während ihres gesamten Lebenszyklus. Dazu gehören die Identifizierung von Schwachstellen, die Implementierung von Sicherheitsmaßnahmen, die kontinuierliche Aktualisierung und die Einhaltung der Secure-by-Design-Prinzipien. Kiteworks unterstützt die Compliance durch seinen Secure Software Development Life Cycle, der interne und externe Tests, Code Reviews, Penetrationstests und Bug Bounty Programme umfasst. Das Unternehmen überprüft die Abhängigkeiten von Drittanbietern, unterhält eine aktuelle Software-Stückliste und führt regelmäßige Schwachstellenanalysen durch. Kiteworks wendet Best Practices wie OWASP-Standards, Least Privilege Access und Defense-in-Depth-Strategien an. Ein dediziertes Sicherheitsteam kümmert sich um die kontinuierliche Bewertung und Behebung von Schwachstellen und gewährleistet ein proaktives Management von Cybersicherheitsrisiken während des gesamten Produktlebenszyklus. Mit diesem Ansatz ist Kiteworks potenziellen Bedrohungen immer einen Schritt voraus, verbessert kontinuierlich die Produktsicherheit

## Highlights der Lösung



**Sicherer Entwicklungs-zyklus**

**Kontinuierliche Tests**

**Standard-einstellungen mit geringsten Rechten**

**Echtzeit-Logging**

**Updates mit einem Klick**

**CISO-Dashboard**

und bietet seinen Kunden robuste, gesetzeskonforme Lösungen, die die strengen Anforderungen des CRA und anderer Cybersicherheitsvorschriften erfüllen.

## Reporting von Vorfällen und Management von Schwachstellen durch Echtzeit-Logging und effiziente Updates

Eine weitere wichtige Gruppe von Kontrollen ist das Schwachstellenmanagement und die Meldung von Vorfällen. Der CRA schreibt strenge Meldepflichten vor, einschließlich der Meldung von Sicherheitsvorfällen oder aktiv ausgenutzten Schwachstellen an die ENISA innerhalb von 24 Stunden nach deren Entdeckung. Kiteworks unterstützt die Einhaltung der Vorschriften mit umfassendem Echtzeit-Logging und der Integration von Security Information and Event Management (SIEM), die eine schnelle Erkennung und Reaktion ermöglicht. Die Plattform unterhält einen kontinuierlichen Schwachstellen-Testzyklus mit automatisierten und manuellen Penetrationstests, Bug-Bounty-Programmen und Audits durch externe Parteien. Das Ein-Klick-Update-System von Kiteworks ermöglicht die schnelle Installation von Sicherheitspatches in geclusterten Umgebungen. Diese Funktionen, kombiniert mit klaren Prozessen für die Offenlegung von Schwachstellen und Verwaltungsmechanismen, ermöglichen es Unternehmen, Cybersicherheitsbedrohungen effizient anzugehen und zu entschärfen und so die Anforderungen des CRA nach zeitnaher Reaktion und Behebung von Schwachstellen zu erfüllen. Die konsolidierten Audit-Protokolle der Plattform erfassen alle sicherheitsrelevanten Aktivitäten lückenlos und bilden eine solide Grundlage für die Analyse von Vorfällen und das Reporting. Darüber hinaus erhöht die für Administratoren mit entsprechenden Berechtigungen einsehbare Software-Stückliste von Kiteworks die Transparenz und erleichtert ein gründliches Schwachstellenmanagement für alle Komponenten und Abhängigkeiten des Produkts.

## Unveränderbare Audit-Protokolle sorgen für lückenlose Dokumentation und Transparenz

Die Dokumentations- und Transparenzkontrollen verlangen von den Herstellern, dass sie eine vollständige technische Dokumentation und klare Benutzeranweisungen zur Verfügung stellen und dass sie sicherstellen, dass die Produkte mit der CE-Kennzeichnung versehen sind, die die Konformität der Produkte mit den Anforderungen des CRA bestätigt. Sie müssen Aufzeichnungen über die Einhaltung der Vorschriften und alle auftretenden Probleme führen und mit den Marktaufsichtsbehörden zusammenarbeiten, indem sie auf Anfrage die erforderlichen Informationen bereitstellen. Diese Maßnahmen unterstützen die Nachprüfbarkeit und ermöglichen eine wirksame Überwachung der Cybersicherheitsverfahren. Die Plattform bietet eine einsehbare Software-Stückliste in der Verwaltungskonsole für autorisierte Administratoren. Kiteworks hält sich an Industriestandards wie NIST CSF und implementiert ein robustes Asset Management, Zugriffskontrollen und Protokollierungsfunktionen. Das System bietet detaillierte Audit-Protokolle, Security Information and Event Management (SIEM) und ein CISO Dashboard für eine effektive Überwachung. Kiteworks dokumentiert sorgfältig den sicheren Software-Entwicklungszyklus und stellt die Verfügbarkeit der erforderlichen technischen Dokumentation und der Benutzeranweisungen sicher. Dieser Ansatz erleichtert die Bereitstellung umfassender Compliance-Aufzeichnungen, fördert die Nachvollziehbarkeit und ermöglicht die Zusammenarbeit mit Marktaufsichtsbehörden. Durch die Bereitstellung klarer, leicht zugänglicher Informationen und die detaillierte Protokollierung hilft Kiteworks Unternehmen, die Transparenzanforderungen des CRA zu erfüllen und die kontinuierliche Compliance nachzuweisen.

Kiteworks bietet eine robuste Plattform, die den Anforderungen des EU Cyber Resilience Act entspricht und ein umfassendes Sicherheitsmanagement für Produkte mit digitalen Elementen bietet. Durch einen sicheren Software-Entwicklungszyklus, kontinuierliche Tests und proaktive Sicherheitsmaßnahmen gewährleistet Kiteworks eine kontinuierliche Risikobewertung und ein kontinuierliches Risikomanagement. Das Echtzeit-Logging, die Integration von SIEM (Security Information and Event Management) und das effiziente Update-System der Plattform unterstützen die schnelle Meldung von Vorfällen und das Management von Schwachstellen. Die einsehbare Software-Stückliste von Kiteworks, die Einhaltung von Industriestandards wie NIST CSF und detaillierte Audit-Protokolle ermöglichen eine umfassende Dokumentation und Transparenz. Diese Funktionen ermöglichen es Unternehmen, die CRA Compliance-Anforderungen zu erfüllen, von Secure Design-Prinzipien bis hin zu Vorfallberichten und gründlicher Dokumentation. Durch die Implementierung von Kiteworks können Unternehmen sicher durch die komplexe Landschaft der Cybersicherheitsvorschriften navigieren, Risiken minimieren und sich einen Wettbewerbsvorteil auf dem EU-Markt verschaffen, während sie gleichzeitig potenzielle Strafen und Reputationsschäden im Zusammenhang mit der Nichteinhaltung von Vorschriften vermeiden.