

SOLUTION BRIEF

Der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) und Armis

Der [Kriterienkatalog C5 \(Cloud Computing Compliance Criteria Catalogue\)](#) ist ein von dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickeltes Rahmenwerk. Es legt strenge Richtlinien für die Sicherstellung von Sicherheit und Compliance in Cloud-Computing-Umgebungen fest. In diesem Solution Brief wird der Kriterienkatalog C5 vorgestellt und erläutert, wie Armis Unternehmen dabei unterstützen kann, diesen Standard zu erreichen und einzuhalten.

Kriterienkatalog C5 - Cloud Computing Compliance Criteria Catalogue

Übersicht über C5

Der Prüfstandard C5 wurde entwickelt, um Cloud-Anbietern und ihren Kunden einen klaren und umfassenden Kriteriensatz zu bieten, um die Sicherheit und Zuverlässigkeit von Cloud-Diensten zu gewährleisten. Die C5-Kriterien sind in mehrere Abschnitte unterteilt, die jeweils verschiedene Aspekte der Cloud-Sicherheit behandeln:

1. Organisation der Informationssicherheit

Legt die Governance und das Management der Informationssicherheit fest.

2. Asset Management

Stellt sicher, dass Assets identifiziert, verwaltet und geschützt werden.

3. Personalressourcen-Sicherheit

Behandelt Sicherheitsmaßnahmen im Zusammenhang mit Personal, das an Cloud-Diensten beteiligt ist.

4. Physische und umweltbezogene Sicherheit

Konzentriert sich auf den physischen Schutz von Datenzentren und Infrastruktur.

5. Kommunikations- und Betriebsmanagement

Befasst sich mit dem Management von Kommunikation und Betriebsverfahren.

6. Zugriffskontrolle

Stellt sicher, dass der Zugriff auf Informationen und Systeme kontrolliert und überwacht wird.

7. Beschaffung, Entwicklung und Wartung von Informationssystemen

Behandelt die Sicherheitsaspekte von System- und Softwareentwicklung.

8. Incident Management

Gibt Richtlinien zur Verwaltung und Reaktion auf Sicherheitsvorfällen vor.

9. Geschäftskontinuitätsmanagement

Konzentriert sich auf die Widerstandsfähigkeit und Wiederherstellung von Dienstleistungen.

10. Compliance

Gewährleistet die Einhaltung der gesetzlichen, behördlichen und vertraglichen Anforderungen.

Bedeutung der C5-Compliance

Die Einhaltung der C5-Anforderungen ist aus mehreren Gründen von wesentlicher Bedeutung:

Vertrauen und Gewährleistung

Zeigt Kunden und Partnern, dass der Cloud-Dienstleister strenge Sicherheitsstandards erfüllt.

Regulatorische Anforderungen

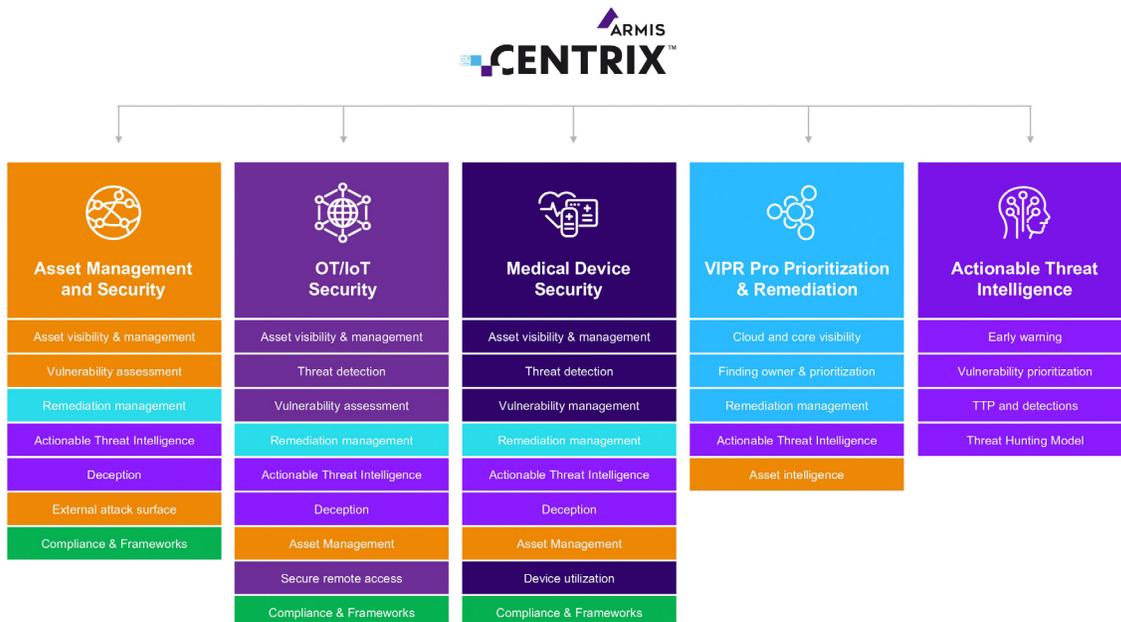
Unterstützt Unternehmen bei der Erfüllung gesetzliche und regulatorische Anforderungen, insbesondere in Deutschland und der Europäischen Union.

Risikomanagement

Verbessert die allgemeine Sicherheitslage durch Identifizierung und Minderung von Risiken, die mit Cloud-Diensten verbunden sind.

Wie Armis bei der C5-Compliance helfen kann

Armis hilft Unternehmen dabei, den Kriterien des C5 im großen Maße gerecht zu werden. Die Armis Centrix™-Plattform bietet eine umfassende Suite von Lösungen, die darauf ausgelegt sind, Organisationen dabei zu helfen, die Einhaltung des C5 Kriterienkatalogs zu erreichen und aufrechtzuerhalten.



Die Schlüsselkompetenzen, die den C5-Kriterien entsprechen, umfassen:

Asset Management

Armis bietet Echtzeiteinblick für alle mit dem Netzwerk verbundenen Assets, einschließlich verwalteter, nicht verwalteter und kurzlebiger Assets in vollem Umfang. Dies entspricht den C5-Kriterien für das Asset Management und stellt sicher, dass alle Assets identifiziert, überwacht und geschützt werden. Mit Armis können Unternehmen:

- | Erkennen und Klassifizieren aller Geräte im Netzwerk, einschließlich Cloud-Assets wie Container, Web-Anwendungen, Workloads, Repositories und mehr.
- | Sicherstellen einer ordnungsgemäßen Asset-Inventarisierung und -Verfolgung.
- | Überwachen Sie Geräteverhalten und identifizieren Sie Anomalien sowie Richtlinienverstöße.

Zugriffskontrolle

Armis hilft bei der Durchsetzung robuster Zugriffskontrollmaßnahmen durch Überwachung und Kontrolle des Netzwerkzugriffs. Dies ist entscheidend für die Erfüllung der C5 Zugriffskontrollkriterien. Armis ermöglicht Unternehmen:

- | Implementierung von Netzwerksegmentierung und Mikrosegmentierung für Assets, die sich nicht wie erwartet verhalten.
- | Sicherer Fernzugriff (Secure Remote Access, SRA) steuert den Zugang zu sensiblen Daten und Systemen nach dem Least-Privilege-Prinzip (PoLP). Mitarbeiter und autorisierte Personen erhalten nur Zugang zu dem, was sie für die Erfüllung ihrer Aufgaben benötigen.
- | Überwachen Sie Benutzerverhalten und Gerätezugriffsmuster.

Sicherheitsresilienz und Behebung

Armis bietet fortschrittliche Funktionen zur Erkennung und Priorisierung von Bedrohungen sowie zur Behebung von Problemen, die alle auf KI basieren. Dies entspricht den C5-Kriterien für Sicherheit und Incident Management, indem sichergestellt wird, dass Unternehmen schnell auf Sicherheitsvorfälle reagieren können. Armis befähigt Unternehmen dazu:

- | Frühzeitige Erkennung von Angriffen, noch in der Entstehungsphase (Frühwarnsystem).
- | Erkennen und Reagieren auf Bedrohungen in Echtzeit.
- | Automatisierung der Alarm-Deduplizierung, -Priorisierung, Incident-Response- und Remediation-Workflows.
- | Integration mit bestehenden Sicherheitssystemen wie SIEM, SOAR und Ticketing-Systemen.

Kommunikations- und Betriebsmanagement

Armis unterstützt das sichere Management von Arbeitsablaufkommunikationen und Betriebsverfahren. Dies ist wesentlich für die Erfüllung der C5-Kriterien für Kommunikations- und Betriebsmanagement. Mit Armis können Unternehmen:

- | Gewährleistung sicherer Kommunikationskanäle.
- | Überwachung des Netzwerkverkehrs auf verdächtige Aktivitäten.
- | Implementierung und Durchsetzung von Sicherheitsrichtlinien.

Compliance und Reporting

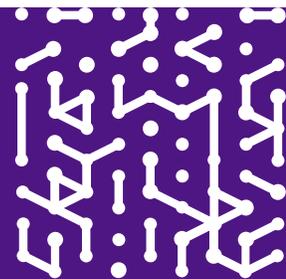
Armis bietet sowohl standardmäßige als auch individuell angepasste umfassende Berichterstattung. Dies hilft Unternehmen, die Kriterien des C5 Katalogs zu erfüllen, indem sie detaillierte Berichte und Prüfungsinformationen zur Verfügung stellen, um der Regulierungsbehörde die Einhaltung der Anforderungen nachzuweisen. Armis bietet:

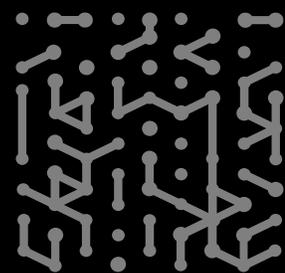
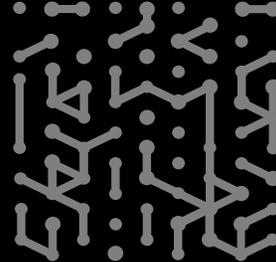
- | Automatisierte Berichterstattung über die Einhaltung der Vorschriften.
- | Detaillierte Audit-Protokolle für alle Aktivitäten sowie eine detaillierte Analyse bestimmter Vorfälle oder Geräte.
- | Durchgehende Überwachung der Compliance-Einhaltung basierend auf den Vorgaben des Unternehmens.
- | Benchmarking, um zu demonstrieren, wie das Unternehmen im Vergleich zu anderen in der Branche abschneidet.

Zusammenfassung

Die Einhaltung des Cloud Computing Compliance Criteria Catalogue (C5) ist für Unternehmen, die Cloud-Dienste nutzen, unerlässlich. Armis Centrix™ ist eine robuste Cybersicherheitsplattform, die mit den C5-Kriterien übereinstimmt und Unternehmen dabei hilft, die Sicherheit und Compliance ihrer Cloud-Infrastruktur sowie der Workloads, die durch sie laufen, zu gewährleisten. Durch die Nutzung von Armis können Unternehmen ihre Sicherheitslage verbessern, regulatorische Anforderungen erfüllen und Vertrauen bei ihren Kunden und Partnern aufbauen.

Für weitere Informationen, wie Armis Ihnen dabei helfen kann die Vorgaben des Kriterienkatalogs C5 einzuhalten, besuchen Sie uns unter armis.com/de oder senden Sie uns eine email an: dach@armis.com.





Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

- Platform
- Industries
- Solutions
- Resources
- Blog

Try Armis

- Demo
- Free Trial

