Anforderungen an Ihren IKT Lieferanten:

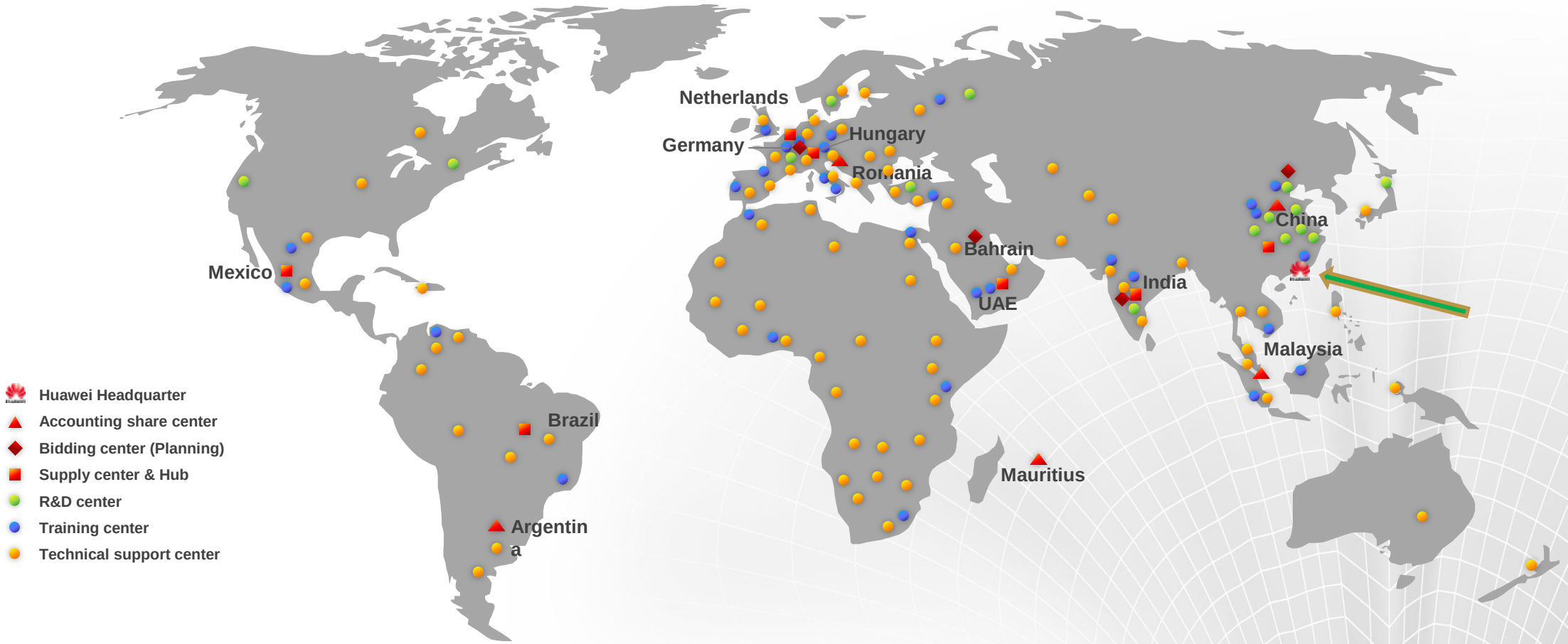
Wo *Ihre* Security Governance beginnen sollte!

www.huawei.com

Ulf Feger / Huawei Technologies
Cyber / Chief Security Officer – Germany
CISSP, CISM, CP (ISACA), ISO27001 PA
ulf.feger@huawei.com

HUAWEI

Unsere globale Verteilung



15 regionale Zentralen, tätig in **140+** Ländern

150.000+ Angestellte mit **150+** Nationalitäten

.. und wie schauts da aus ?

Cyber Security White Boarding" - on a napkin"

Agenda

Was soll’s denn sein – 50 Gramm mehr?
Die Sicherheitsherausforderung?
Was sind die Top 100?

Cyber Security White Boarding" - on a napkin"

Die Sicherheitsherausforderung?

Sie interessieren sich für Anwendung oder Erwerb von IKT-Produkten?

Einer der wichtigsten Faktoren in diesem Zusammenhang ist die Frage nach der Sicherheit meiner Produkte. Oft wird dabei von Security Governance oder Produktsicherheitszertifikaten gesprochen.

- Wie kann ich sicher gehen, dass der jeweilige IKT-Hersteller/Lieferant auch meinen komplexen Unternehmensanforderungen entspricht?
- Welche Fragen sollte ich vorab klären?
- Welche Antworten sollte mir ein Anbieter liefern können?

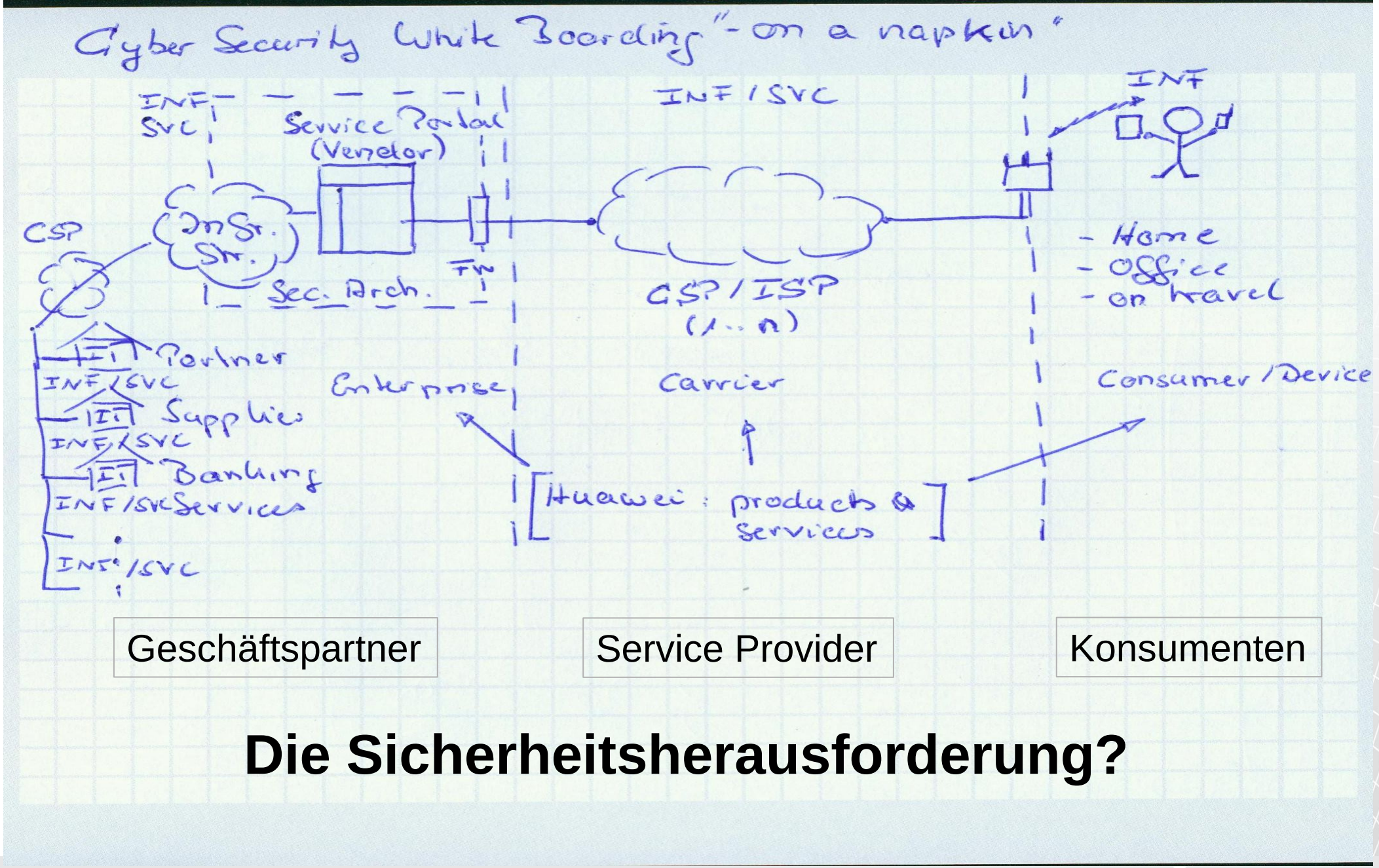
Basierend auf jahrelanger Expertise und praktischer Umsetzungserfahrung stellt Ihnen Huawei einen umfangreichen Fragenkatalog zum Thema IKT vor.

Cyber Security White Boarding" - on a napkin"

Worin besteht die Sicherheitsherausforderung für Kunden, Hersteller und Lieferanten?

- vom Standpunkt eines Sicherheitsverantwortlichen (CISO/CSO)?
- vom Standpunkt einer Risikobetrachtung?
- vom Standpunkt eines Einkäufers?
- vom Standpunkt eines Integrators / Dienstleiters / Beraters?
- von ... ?

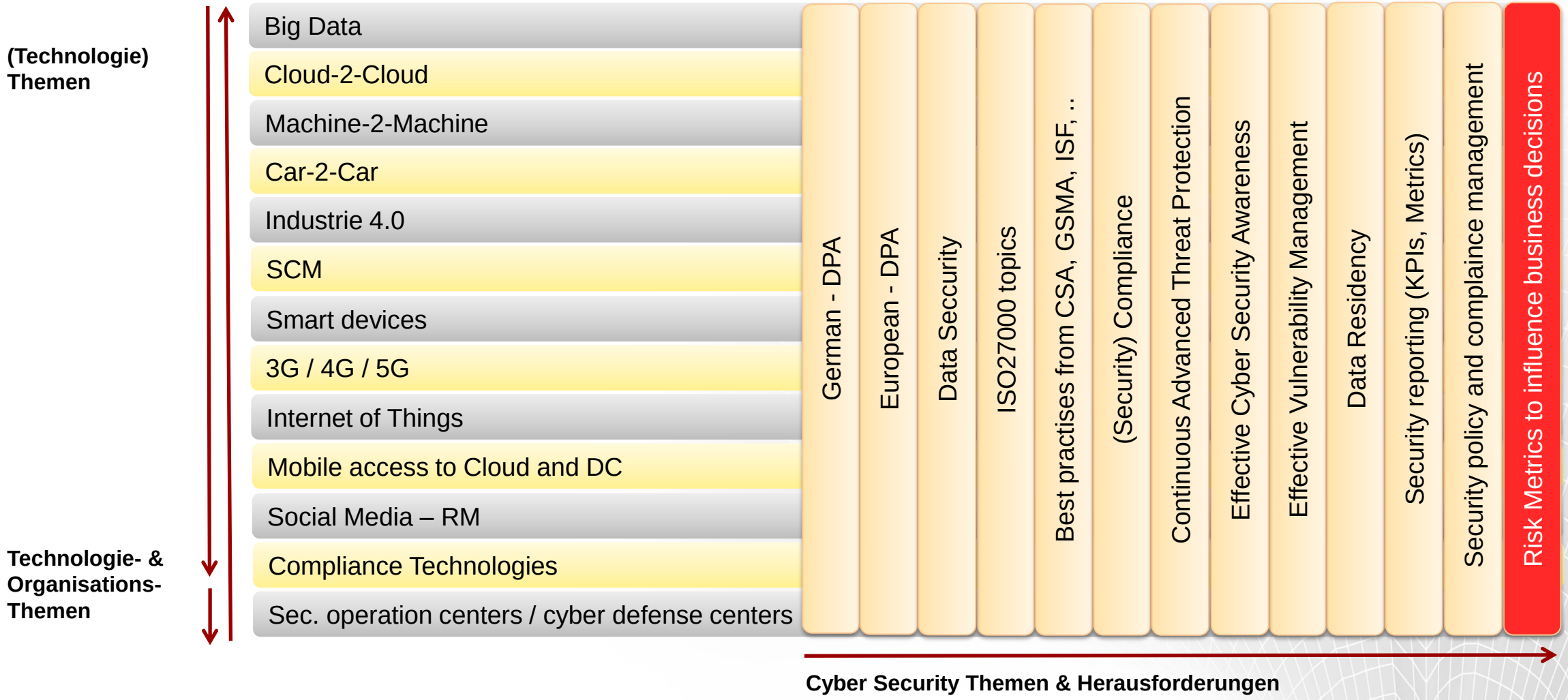
Cyber Security White Boarding" - on a napkin"



Geschäftspartner | Service Provider | Konsumenten

Die Sicherheitsherausforderung?

Veränderungen, Herausforderungen und Chancen



Cyber Security White Boarding" - on a napkin"

Neben der technischen Expertise…

Auf welcher Basis kann ich entscheiden, ob mein Hersteller / Lieferant / Dienstleister ein vertrauenswürdiger Lieferant ist?

Welchen Leitfaden kann ich hierfür nutzen?

Top 100

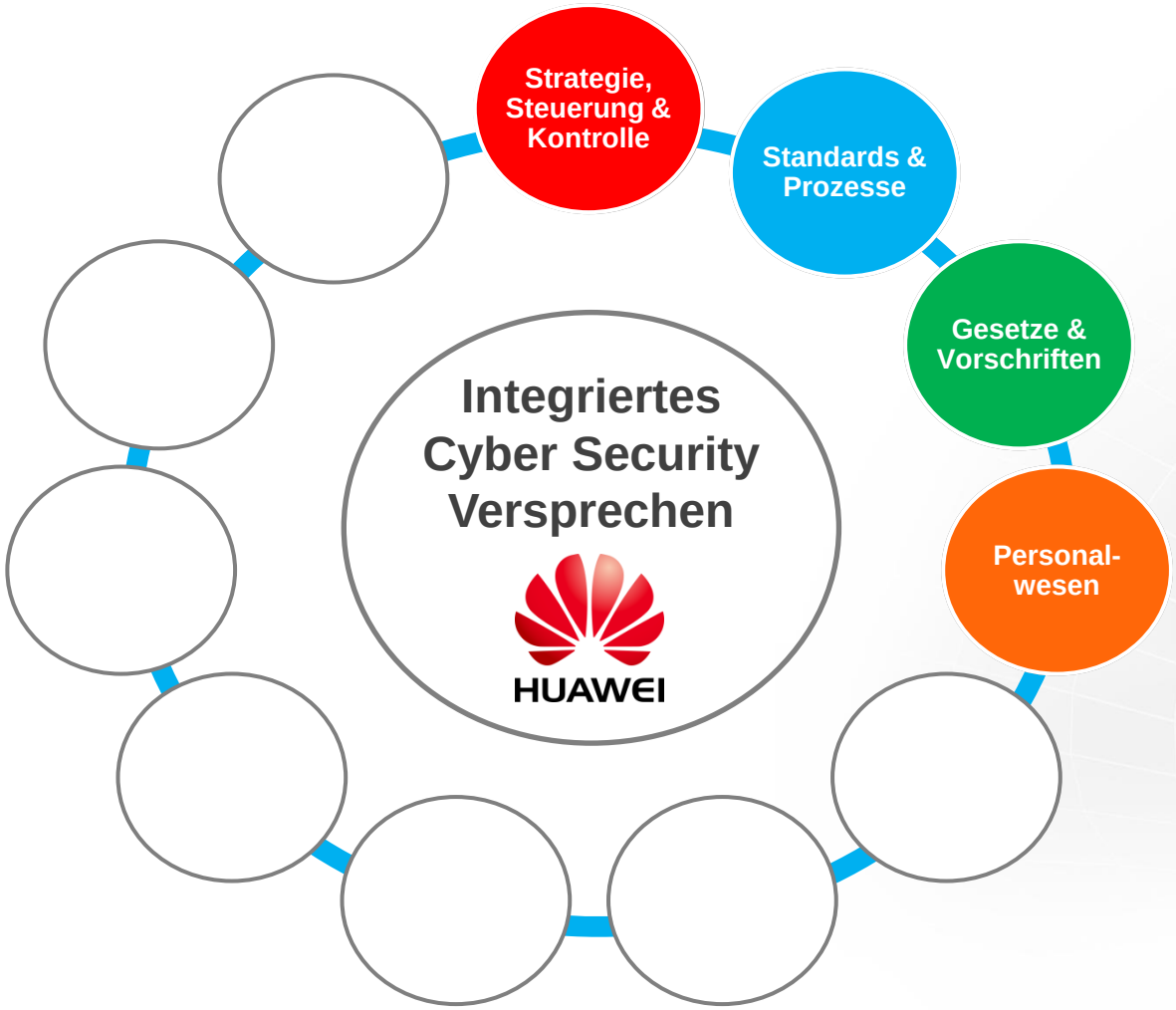
In der Ausarbeitung der Top 100 haben wir vielfältige Quellen genutzt.
Wir haben unseren Kunden intensiv zugehört:

- Was sind ihre größten Probleme?
- Worüber sind sie beunruhigt?
- Wo liegen ihre Zweifel?
- Was sind ihre Anforderungen?
- Welche Anforderungen der Industrie und der jeweiligen Länder existieren?

Als einer der führenden Hersteller der IKT Industrie decken wir fast alles von Telekommunikationsinfrastruktur bis Cloud Compunting sowie Enterprise- und Endverbraucher-Lösungen ab.

Daher haben wir letzendlich über 1200 Standards, Artikel, Best und Good Practises durchsucht, um einen gewissen Grad an Konsitenz zu erreichen.

Sicherheits-Kontroll-Punkte des E-zu-E Systems



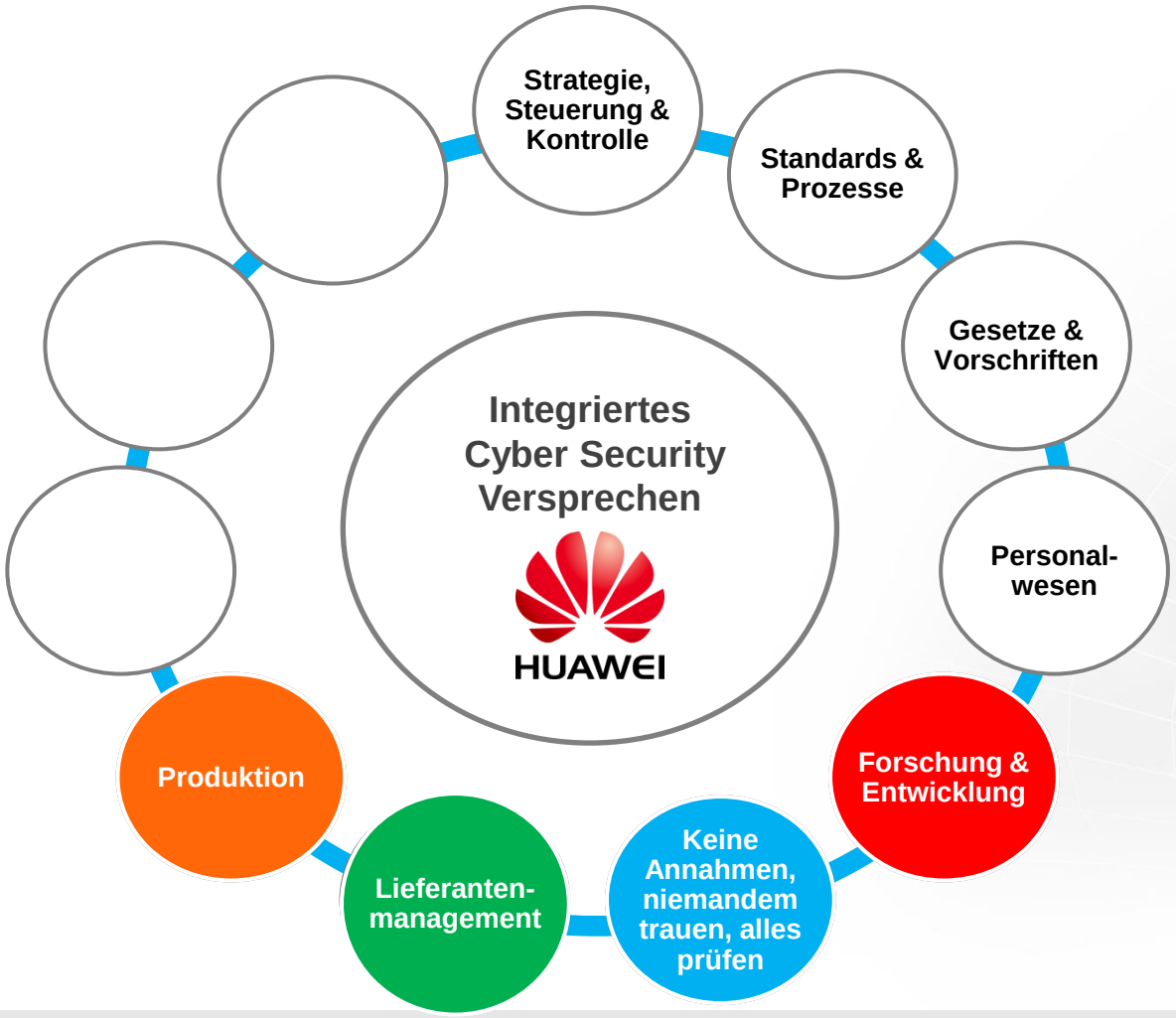
Klare, formale und offene Strategie: Die Cyber Security steht über geschäftlichen Interessen.
Angemessene Steuerungsstruktur: Top-down-Betonung der Wichtigkeit von Cyber Security; Gründung eines globalen Ausschusses für Cyber Security; Effektive Kontrollmethoden: Ende-zu-Ende Sicherungssystem; Integrierung von Cyber Security in Prozesse.

Übernehmen und Unterstützen internationaler Standards und Beitritt in Normenorganisationen und -gruppen zur Einführung von Grundanforderungen für Geschäftsaktivitäten durch Integrierung externer Standards, Best Practices und Anforderungen. Integrierung von Cyber Security in Geschäftsabläufe zur Sicherstellung der Beständigkeit gelieferter Produkte und Services in überschneidenden Geschäftsaktivitäten.

Die Gesetzgebung zur Cyber Security spiegelt die strategischen Anforderungen eines Landes zur Cyber Security wider. Es ist notwendig, die Gesetze zur Cyber Security vollständig zu verstehen und bei Geschäftsaktivitäten einzuhalten, um rechtliche Risiken zu vermeiden.

Bewusstsein und Fähigkeiten jedes Angestellten hinsichtlich Cyber Security zu schärfen ist die Basis. Stärkung des Managements hinsichtlich wesentlicher Aspekte der Cyber Security zur Minimierung interner Risiken.

Sicherheits-Kontroll-Punkte des E-zu-E Systems



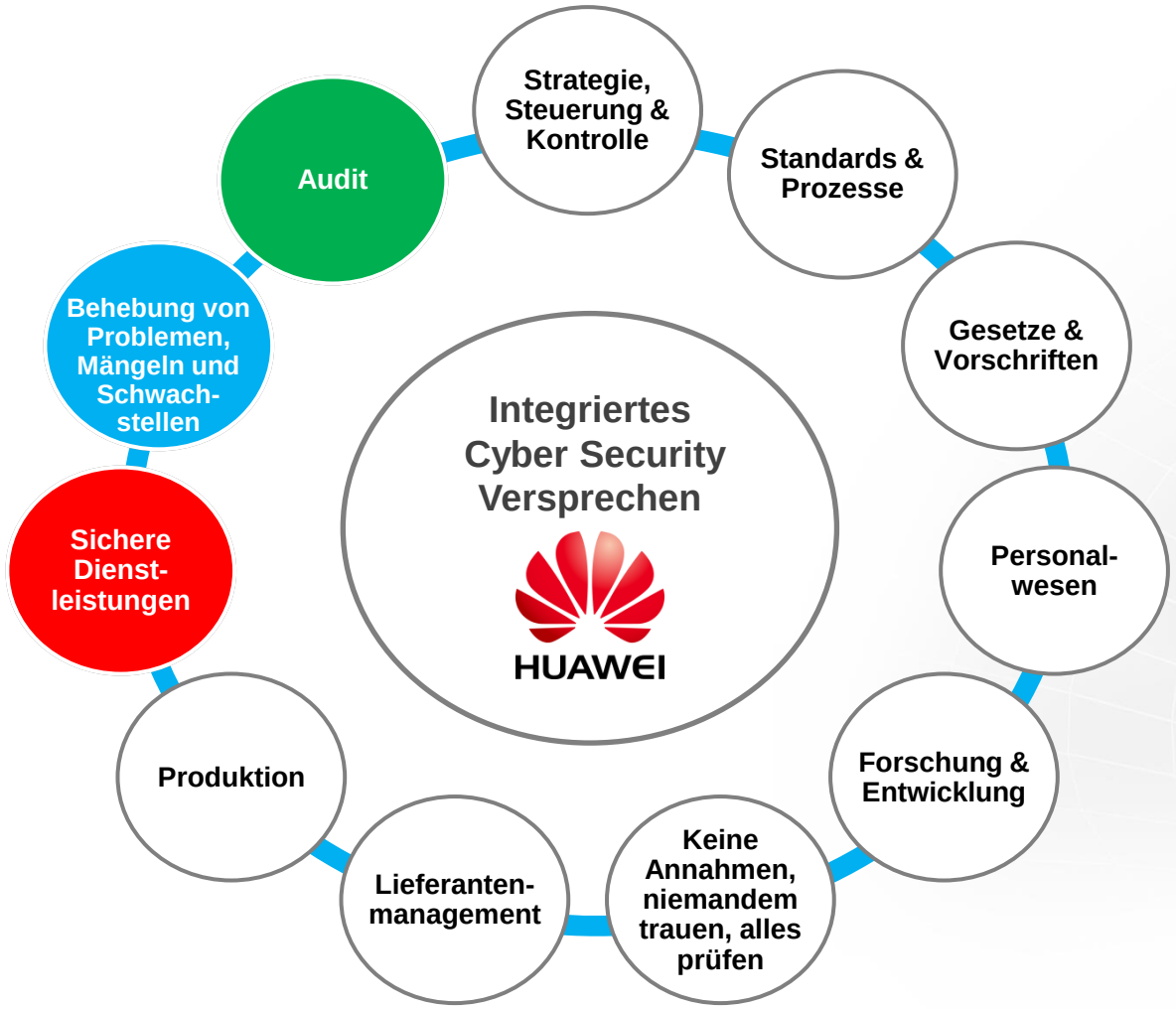
Integrierung von Cyber Security-Anforderungen und -maßnahmen in **Produktforschungs- und Entwicklungsprozesse** zur Gewährleistung der Produktsicherheit in gleichem Maße wie der Produktqualität.

Produktsicherheit kann nicht einzig durch Prüfung garantiert werden. Dennoch senkt eine **mehrstufige unabhängige Überprüfung** außerhalb von Forschung und Entwicklungsprozessen das Risiko, dass unsichere Produkte in den Handel kommen. Somit sind Investition des Kunden sowie Services besser geschützt.

Die Integrierung externer Ressourcen des Marktes konfrontiert jedes Unternehmen mit Risiken. Ein offizieller **Beschaffungsprozess** und **Bewertungsmechanismus** können solche Risiken minimieren und zwar durch Sicherstellung, dass Managementansätze und Leistungen des Drittanbieters den Anforderungen entsprechen.

Aufnahme risikominimierender Maßnahmen in alle Prozesse – von der **Herstellung** und **Logistik bis hin zu Rückführung**. Diese Maßnahmen bieten drei vorbeugende Funktionen in der Herstellung (Anti-Manipulation, Anti-Implantation und Anti-Fälschung) zur Gewährleistung der Durchgängigkeit in dreierlei Hinsicht (zwischen Eingangsmaterialien und Beschaffungs-anforderungen, zwischen Produktsoftware und -hardware und deren F&E-Anforderungen und zwischen Produktlieferungen und Kundenan-forderungen) und bieten notwendige **Rückverfolgbarkeit**. Unser Ziel ist es, dass unsere Produkte im Einklang mit den Kundenanforderungen stehen.

Sicherheits-Kontroll-Punkte des E-zu-E Systems

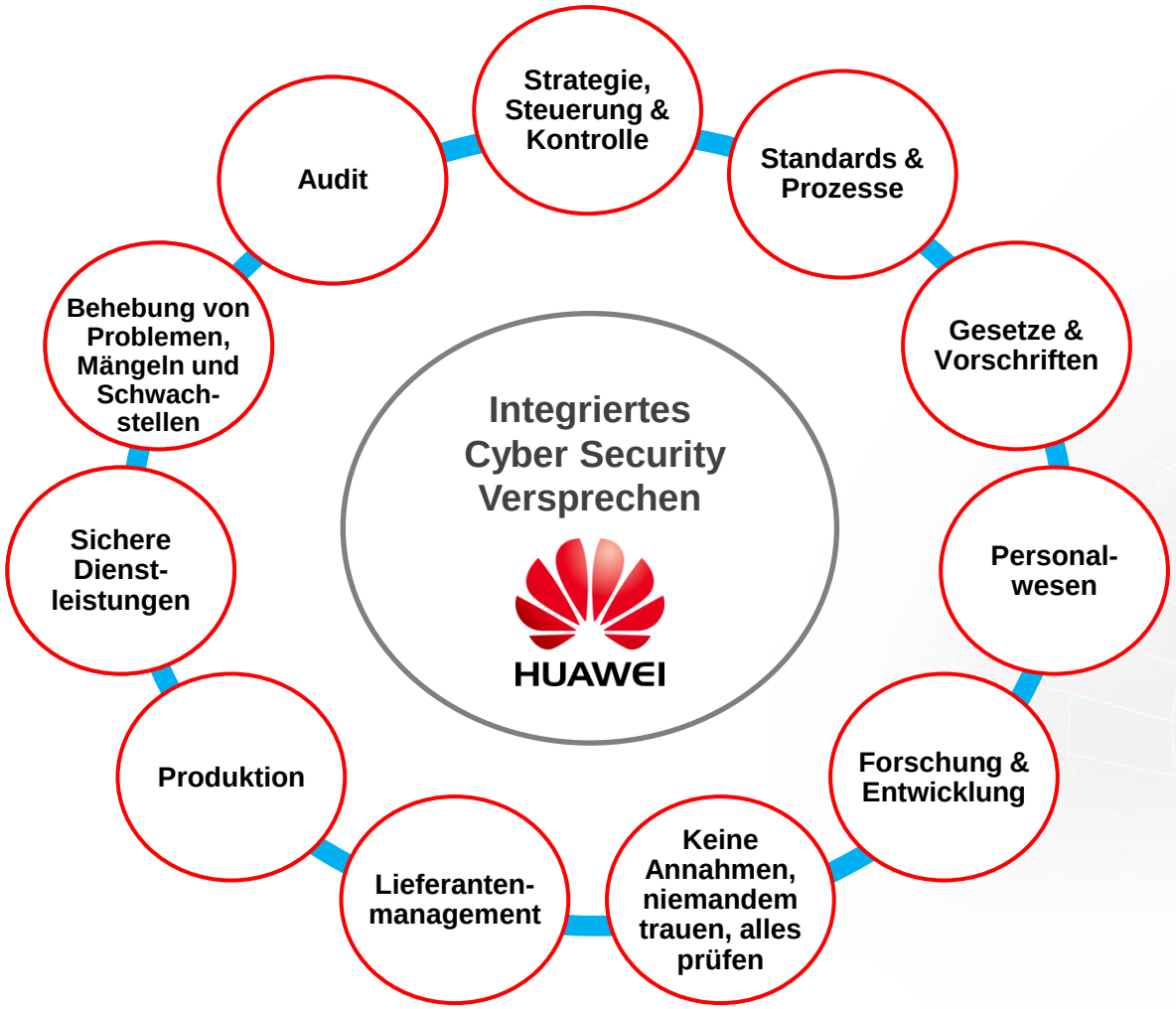


Während des langen **Prozesses des Betriebs** von Erzeugnissen muss sich das Geschäft fortlaufend weiterentwickeln und ausreichende **Maßnahmen** zur Risikominimierung bieten (z.B. Datenverlust und Cyber-Angriffe), die durch Expansion und Anpassungen verursacht werden und so die Geschäftskontinuität gewährleisten. Bei der Lieferung und Betreuung von Produkten ist es entscheidend, **bestehende Lieferprozesse und -regeln einzuhalten** sowie Zusammenhänge und Betriebsabläufe zu kontrollieren.

Beim Thema Sicherheit gibt es keine 100 %-ige Garantie. Probleme zu **verhindern** und ihre **Auswirkungen zu reduzieren** ist abhängig von optimalen Mechanismen, professionellen Organisationen und effizienten Prozessen, die auf Sicherheitsprobleme reagieren. Zur Gewährleistung der Stabilität muss sich eine Organisation auf ein professionelles **Product Security Incident Response Team (PSIRT),** effektive **Prozesse** zur Problemlösung und Reaktions-vermögen sowie eine enge Zusammenarbeit mit dem Computer Security Incident Response Team des Kunden verlassen.

Worten Taten folgen lassen, um Kunden von der Sicherheit der Produkte und Services zu überzeugen. Offen bleiben für interne Prüfanforderungen sowie externe Prüfanforderungen von Kunden und Dritten. Strenge Prüfungen durchlaufen zur Sicherstellung der vollständigen Einhaltung aller geltenden Bestimmungen, Verfahren und Standards und zur Lieferung von gewünschten Geschäftsergebnissen.

Sicherheits-Kontroll-Punkte des E-zu-E Systems



Bereich	Schwerpunkt
Strategie, Steuerung und Kontrolle	Eine übergreifende Strategie sowie die Verantwortung haben, diese umzusetzen
Standards und Prozesse	Einsatz der besten Standards und Vorgehensweisen zum Schutz vor Bedrohungen und Risiken
Gesetze und Vorschriften	Die Produkte und Abläufe entsprechend den Gesetzen der jeweiligen Länder konform gestalten
Personalwesen	Zur Minimierung von Insiderproblemen die richtigen Stellen mit den richtigen Personen mit den richtigen Verhaltensweisen besetzen
Forschung und Entwicklung	Produkte auf eine sichere Weise, die auf den obigen Leitlinien basiert, entwerfen, herstellen und testen
Prüfung: keine Annahmen, niemandem trauen, alles prüfen	Viele Augen, viele Hände, viele Prüfungen. Mehrstufiges unabhängiges Vorgehen bei der Sicherheitsüberprüfung
Lieferantenmanagement	Sensibilisierung der Lieferanten, die Sicherheit ernst zu nehmen
Produktion	Herstellen von Produkten, die helfen jeden Schritt abzusichern – bis hin zur Lieferung
Sichere Dienstleistungen	Installation, Service und Kundendienst zuverlässig gesichert. Keine Manipulationen, vollständig überprüfbar
Behebung von Problemen, Mängeln und Schwachstellen	Sobald Probleme auftreten, diese schnell lösen und dafür sorgen, dass die Technologie des Kunden gesichert ist
Audit	Einsatz strenger Prüfmechanismen, um sicherzustellen, dass jeder Teil von Huawei diese Strategie einhält

Top 100

http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm

Nr.	Art	Inhalt	Anzahl
1	**Strategie, Steuerung und Kontrolle**	Die Führungsspitze räumt der Cyber Security eine große Bedeutung ein und besitzt formale Strategien zur Cyber Security. Diese sind in Unternehmensführung, Organisationsstruktur und internem Kontrollrahmen verankert, um die Durchführung der Strategien zu unterstützen.	**8**
2	**Standards und Prozesse**	Einhaltung ausgewiesener weltweit anerkannter Standards, um gleichbleibende Ergebnisse durch Prozessabsicherung zu erzielen.	**3**
3	**Gesetze und Vorschriften**	Die Anforderungen der Cyber Security, der Gesetze und Vorschriften vollständig verstehen und einen Mechanismus besitzen, um Konflikte zwischen einzelnen Anforderungen zu lösen und so für die Einhaltung zu sorgen.	**7**
4	**Personalwesen**	Die Bewusstseinsbildung für Cyber Security erstreckt sich sowohl auf das Führungsteam als auch auf Subunternehmer. Es besteht ein Mechanismus, entscheidende Positionen für die Cyber Security zu schaffen und Fähigkeiten zu verbessern.	**10**
5	**Forschung und Entwicklung**	Basierend auf den Best Practices der Branche nimmt das Unternehmen Anforderungen zur Cyber Security in ihre Forschungs- und Entwicklungsprozesse auf. Die Organisation bringt denselben Stellenwert ebenso Dritten und dem Management von Open Source Software entgegen.	**21**
6	**Prüfung**	Dem Gedanken „Keine Annahmen, Niemandem trauen, Alles prüfen" folgen. Zudem ein unabhängiges Prüfungssystem mit „vielen Augen" unterstützen.	**11**
7	**Lieferanten-management**	Ein offizieller Beschaffungsprozess sowie Bewertungsmechanismus, um sicherzustellen, dass sowohl Management als auch die Lieferung Dritter die Anforderungen einhalten.	**8**
8	**Produktion**	Mechanismen zur Risikominimierung in der Produktsicherheit bei Produktion, Logistik, Rückwärtslogistik usw..	**15**
9	**Sichere Dienst-leistungen**	Bei der Lieferung von Produkten und der Betreuung von Kunden muss die Organisation die geltenden Lieferprozesse und Regeln konsequent einhalten.	**11**
10	**Behebung von Problemen, Mängeln und Schwachstellen**	Vorhandensein eines professionellen PSIRT Teams und eine effektive Abwicklung sowie Reaktionsfähigkeit bei Problemen, Mängeln und Schwachstellen.	**4**
11	**Audit**	Lieferanten sollen Prüfungsvorschriften interner Art, von Kunden oder Dritten gegenüber offen sein. Strenge Prüfungen stellen die korrekte Anwendung von Richtlinien, Verfahren und Standards sicher, um gewünschte Geschäftsergebnisse zu liefern.	**2**
Gesamt			**100**

http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm

Für Sie – bitte nutzen!

Wie gewährleistet Huawei Cyber Security: Alle Antworten zu diesem Thema finden Sie in den von uns veröffentlichten White Papers

Cyber Security White Paper 1 (09/2012)

Beschreibt Huaweis Einstellung zum Thema Cyber Security und die Unabhängigkeit des Unternehmens.

Cyber Security White Paper 2 (10/2013)

Beschreibt die E2E Cyber Security-Prozesse und Praktiken, um die Offenheit von Huawei zu zeigen.

Cyber Security White Paper 3 (03/2014)

Beschreibt Huaweis bisherige Bemühungen und Stimmen im Bereich Cyber Security-Standards.

TO BE

Cyber Security White Paper 4 (TBA)

Wird den Einfluss von Cyber Security auf zukünftige Technologie-Trends beschreiben.

Ulf Feger / Huawei Technologies
Cyber / Chief Security Officer – Germany
CISSP, CISM, CP (ISACA), ISO27001 PA
ulf.feger@huawei.com

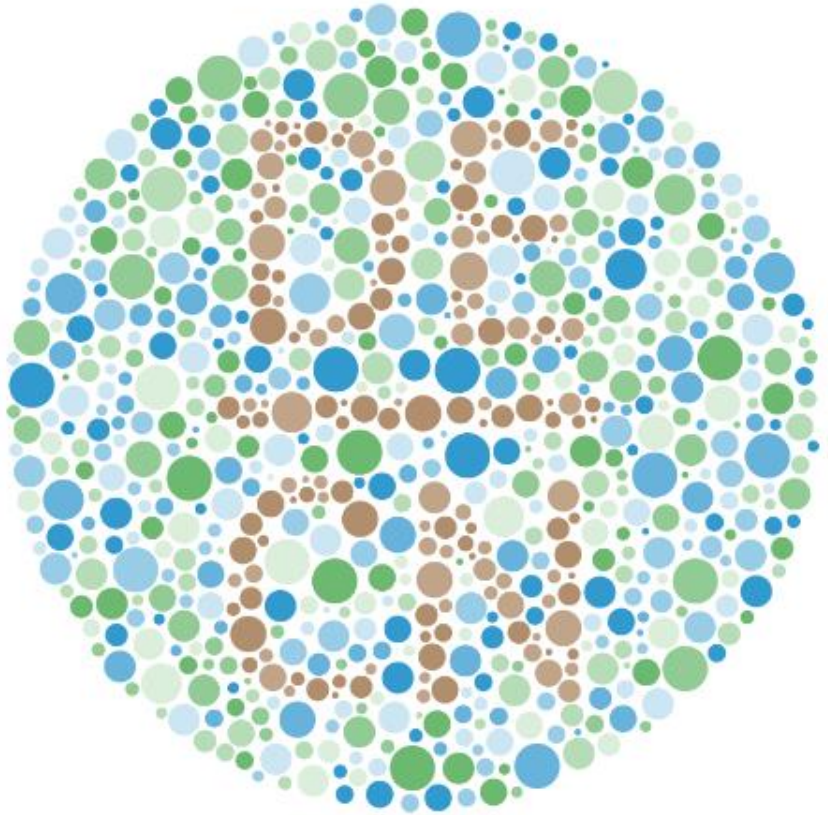
Danke für Ihre Aufmerksamkeit!

www.huawei.com

Wahrnehmung und Realität

http://www.huawei-studie.de
http://www.huawei-studie.de/download

Deutschland und China – Wahrnehmung und Realität
Die Huawei-Studie 2014



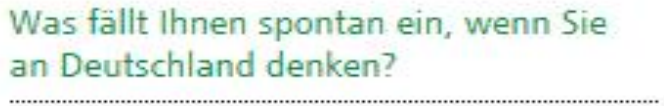
In Zusammenarbeit mit
GIGA German Institute of Global and Area Studies
und TNS Emnid

Verfügbar:

- Deutsch
- Englisch
- Chinesisch

Perzeption und Realität

Top 5:



n. e. = nicht erhoben (Angaben in Prozent, Mehrfachantworten)

n. e. = nicht erhoben (Angaben in Prozent, Mehrfachantworten)