

# Modern információs és kommunikációs technológiák: mi tesz egy ellátási láncot biztonságossá?

**Cserhádi Vencel**

Kiberbiztonsági és adatvédelmi vezető, Huawei Technologies Hungary

Budapest, 2024. január 17.



# Miért kell különösen figyelni az ellátási lánc kockázataira?

A jelenlegi **geopolitikai kontextusban** az ellátási lánc kockázatkezelésének nagy jelentősége van

A **digitalizáció** és az új technológiák megváltoztatják az ellátási lánc hagyományos struktúráját

A Huawei-nek sokrétű tapasztalata van az ellátási lánc kockázatairól és az azok kezelésére szolgáló **jó gyakorlatokról...**

What do Red Sea assaults mean for global trade?

3 days ago

Israel-Gaza war



Subscribe  
Search  
Legal & Compliance

**Build a Resilient Supply Chain Amid U.S.-China Trade War**

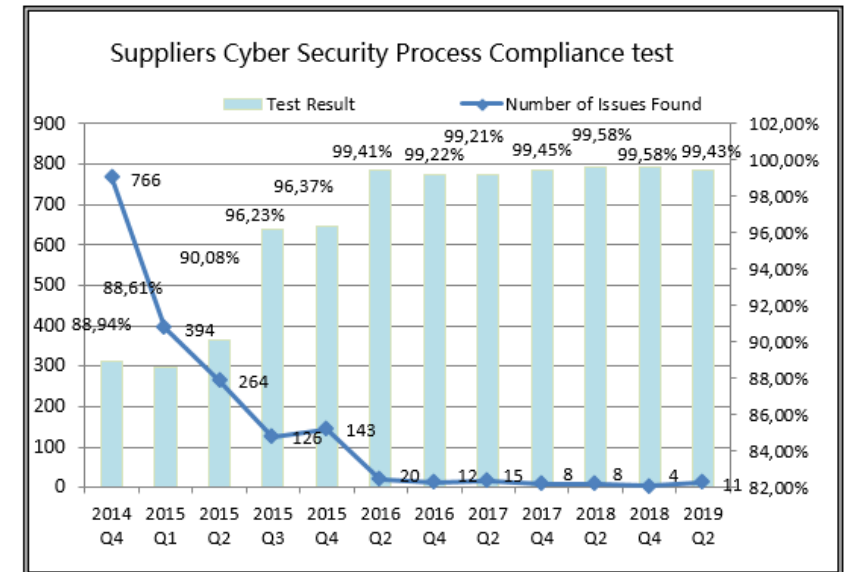
Supply Chain



Companies that embrace new predictive analytics and data science will increasingly outstrip their competitors – but getting there won't be easy.

**The impact of 5G: How will 5G affect supply chain & logistics?**

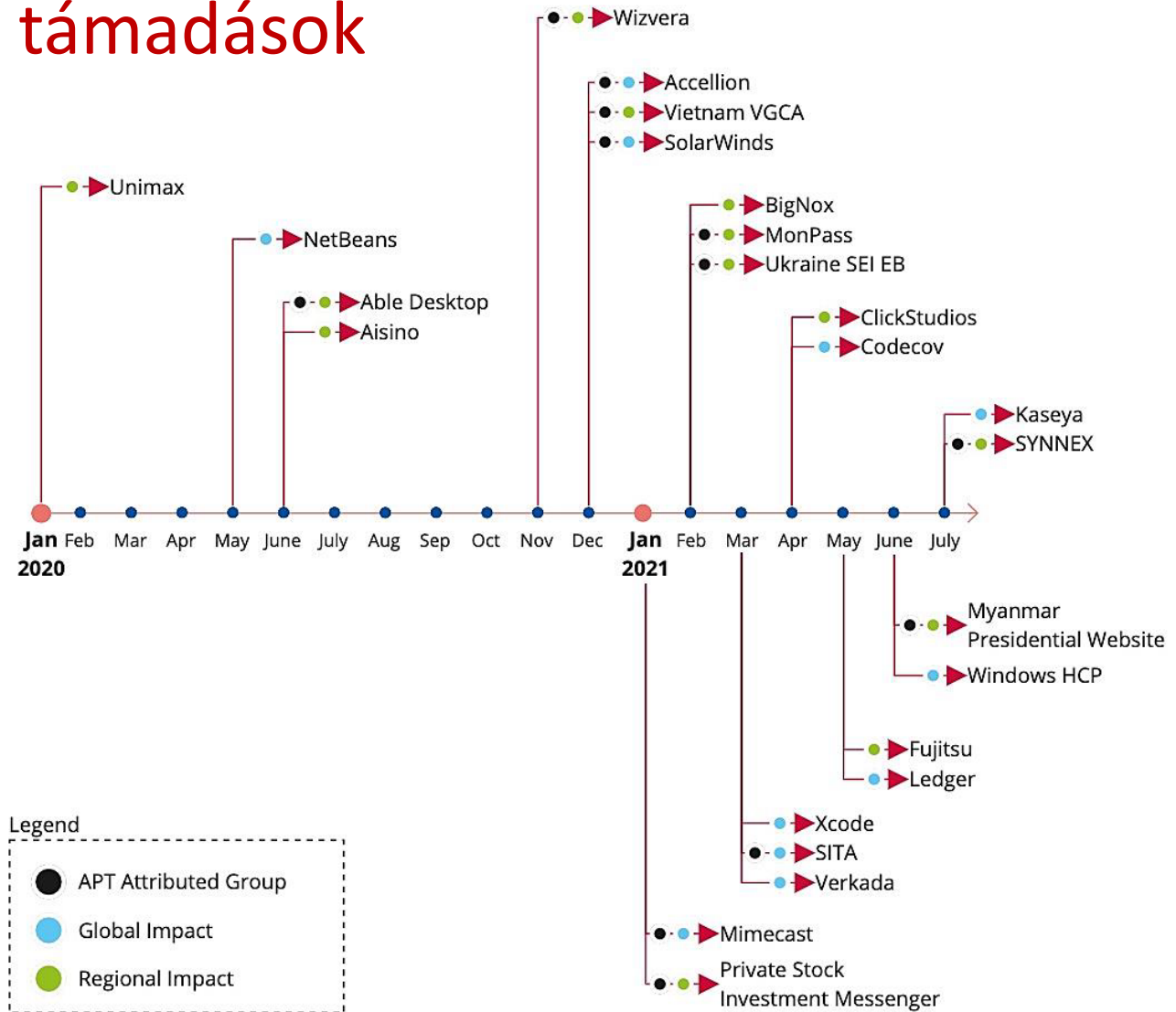
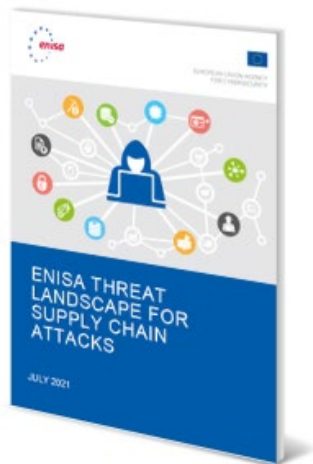
Supply chain and logistics involve a lot of moving parts



# Az ellátási láncok elleni támadások

## ENISA:

"Az ellátási láncot érő támadások már évek óta biztonsági problémát jelentenek, de úgy tűnik, hogy 2020 óta a közösség egyre több, szervezettebb támadással néz szembe."



Forrás: ENISA fenyegetettségi térkép az ellátási lánc elleni támadások tekintetében

# A támadások már egy ideje léteznek...

Az NSA olyan megfigyelőberendezésekkel látta el a Cisco útválasztóit, amelyek elfogják az ezen eszközök által kezelt forgalmat, és átmásolják azt az NSA hálózatára.



Egy Siemens-alvállalkozó rosszindulatú kóddarabokat, úgynevezett logikai bombákat helyezett a szoftverbe



A hackerek kódalírási tanúsítványokat loptak a D-Link-től, és ezeket a kódokat a PC-kről jelszavakat lopó rosszindulatú szoftverek terjesztésére használták.



A hackerek a SolarWinds Orion szoftverének kompromittált frissítése révén jutottak be különböző amerikai kormányzati és egyéb rendszerekbe.

2014

2015

2016

2017

2018

2019

2020



Az XcodeGhost malware 39 iOS alkalmazást fertőz meg, köztük a WeChatet is



A hackerek képesek voltak csapdába csalni az Avast által kínált CCleaner eszközt, hogy távolról telepítsenek egy hátsó ajtó-implantátumot számítógépek millióira.



Roszindulatú kódot építettek be a Juniper NetScreen operációs rendszerébe, amely lehetővé tette a távoli rendszergazdai hozzáférést és a VPN-forgalom passzív visszafejtését.



# Az ellátási lánc fő fenyegetései

Érintett felek Fenyegetések	Módosított termék			Hamisítvány		
	Upstream	Szolgáltató	Downstream	Upstream	Szolgáltató	Downstream
Malware	✓	✓	✓			
Engedély nélküli "alkatrészek"	✓	✓	✓	✓		
Jogosulatlan konfiguráció			✓			
Nem szabványos, selejtezett alkatrészek használata				✓		
Engedély nélküli gyártás				✓		✓

Forrás: [Open Trusted Technology Provider™ Standard \(O-TTPS\) - A rosszindulatúan módosított és hamisított termékek csökkentése: 1. rész: Követelmények és ajánlások](#)

Bizalmasság

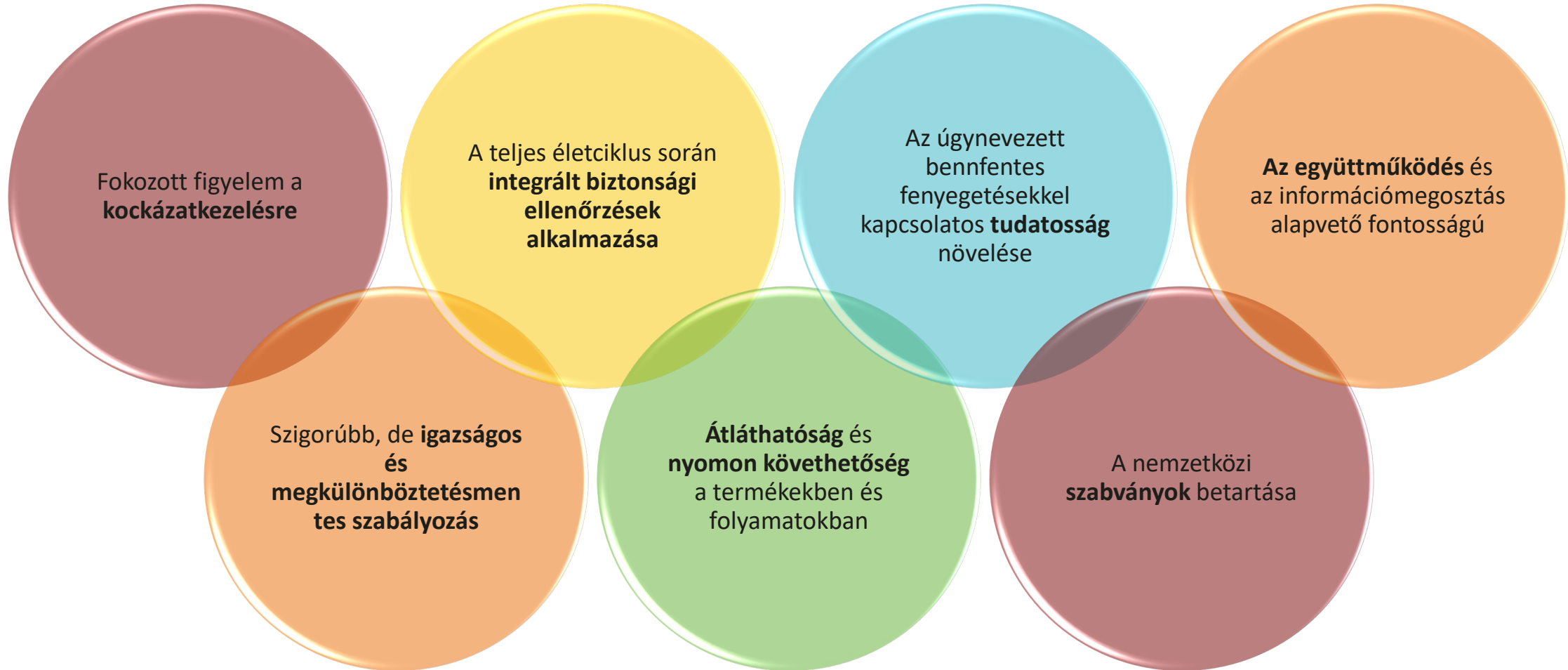
Integritás

Elérhetőség

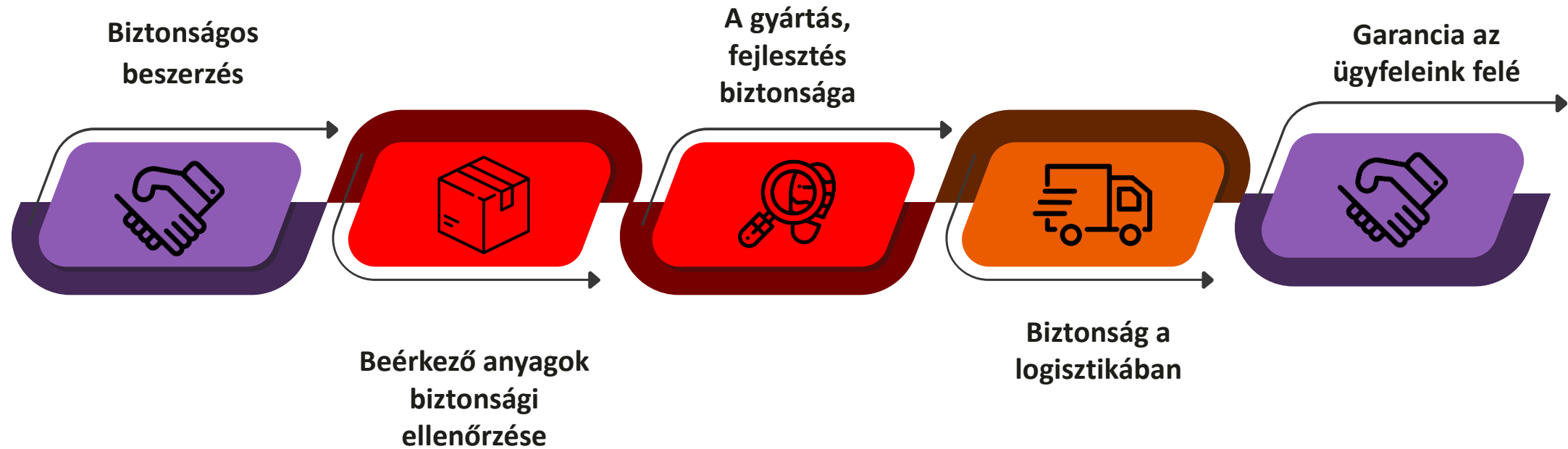
Nyomonkövethetőség

Eredetiség

# A biztonsági kockázatokat minimalizálni kell



# A Huawei megközelítése a biztonságos ellátási láncért



# Kiberbiztonsági intézkedések a beszerzésben

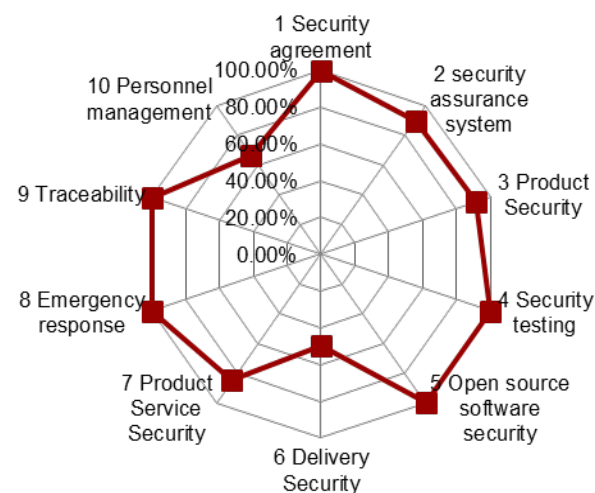
Szállító neve	XXX	Auditálás dátuma	XXX
Ellenőrzött hely	XXX	Kapcsolattartó személy és cím	XXX
Vezető auditor	XXX	Könyvvizsgáló	XXX

Nem.	szakasz	Súly	Százalékos arány	Súlyozott pontszám	Megjegyzések
1	Kiberbiztonsági megállapodás	7%	100.00%	7.0%	
2	Kiberbiztonsági rendszer	12%	92.86%	11.1%	
3	Termékbiztonság	18%	92.86 %	16.7%	
4	Biztonsági tesztelés	20%	88.89%	17.8%	
5	3 <sup>rd</sup> fél szoftverek biztonsága	6%	83.33%	5.0%	
6	Szállítási biztonság	5%	62.50%	3.1%	
7	Szolgáltatás biztonsága	5%	95.00%	4.8%	
8	Vészhelyzeti reakcióterv	15%	93.75%	15.0%	
9	Nyomonkövethetőség	5%	90.00%	4.5%	
10	Személyzet tudatosítása	6%	87.67%	5.3%	
Összesen			90.26%		
Fokozat			Kiváló		

Beszállítói kiberbiztonsági és adatvédelmi rendszer minősítési szabványok és ellenőrző lista V2.0

1. Kiberbiztonsági és adatvédelmi megállapodás
2. Meglévő beszállítók éves auditálása
3. Kritikus beszállítók műszaki értékelése

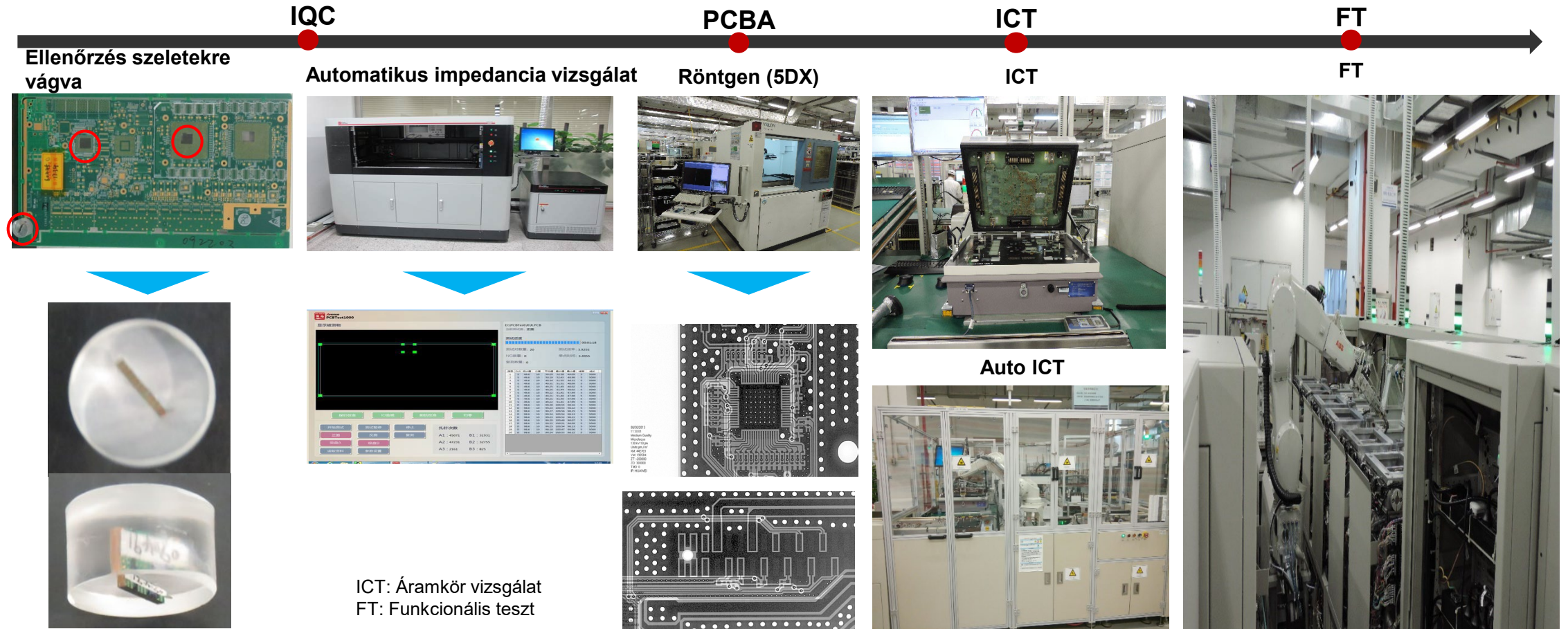
Ez az ellenőrzési lista **10 elemet, 42 kérdést** tartalmaz, amelyek mindegyike az összpontszám 5%-15%-át teszi ki. Az egyes tételek 1-10 kérdést tartalmaznak a szállító kiberbiztonságának értékelésére.



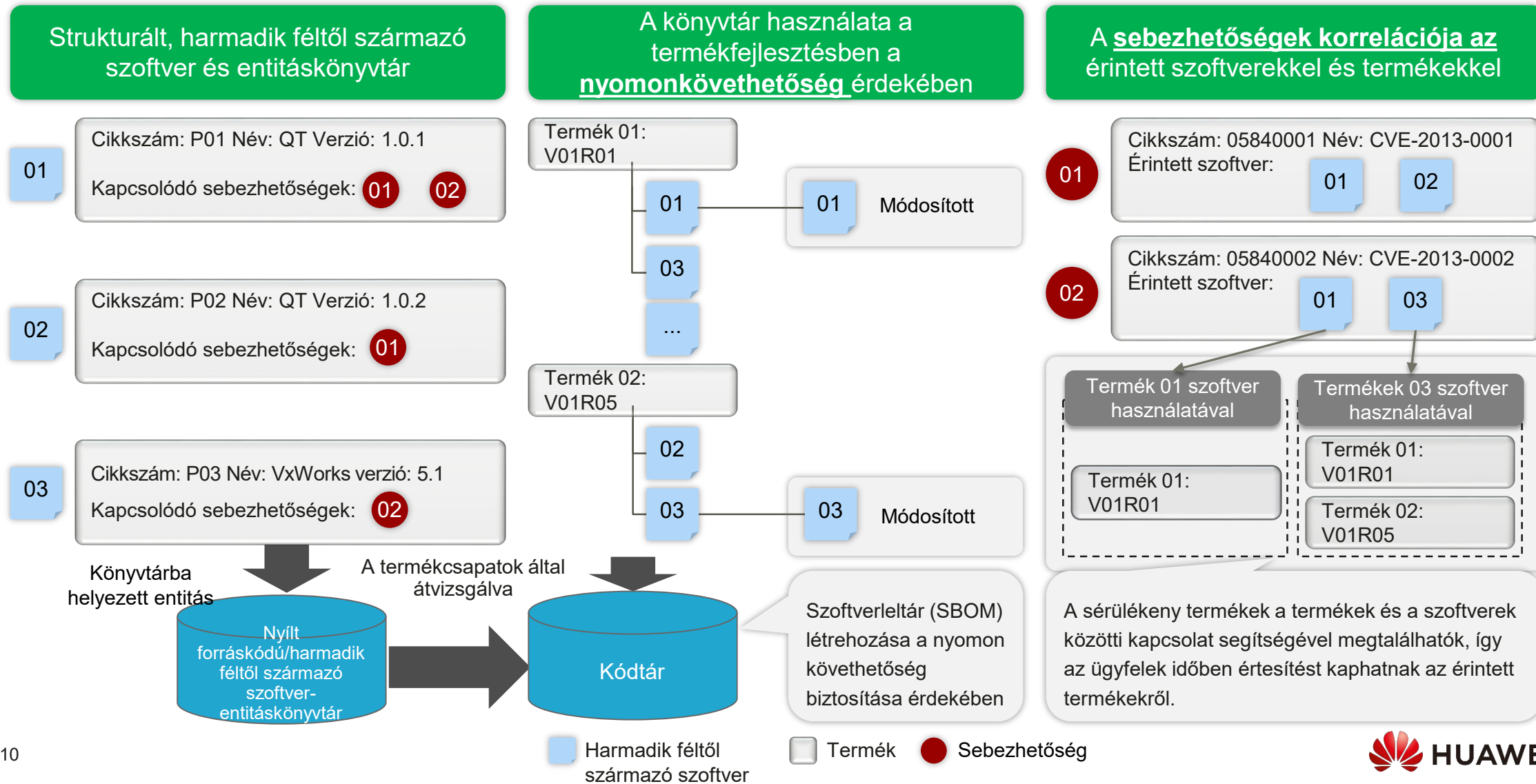
Weighted score	Grade	Risk level
<70%	D Failure	High risk
≥70%	C Conditional Pass	Medium risk
≥80%	B Good	Low risk
≥90%	A Excellent	Benchmark



# Beérkező anyagok: minden egyes beszállítói tétel alapos vizsgálata

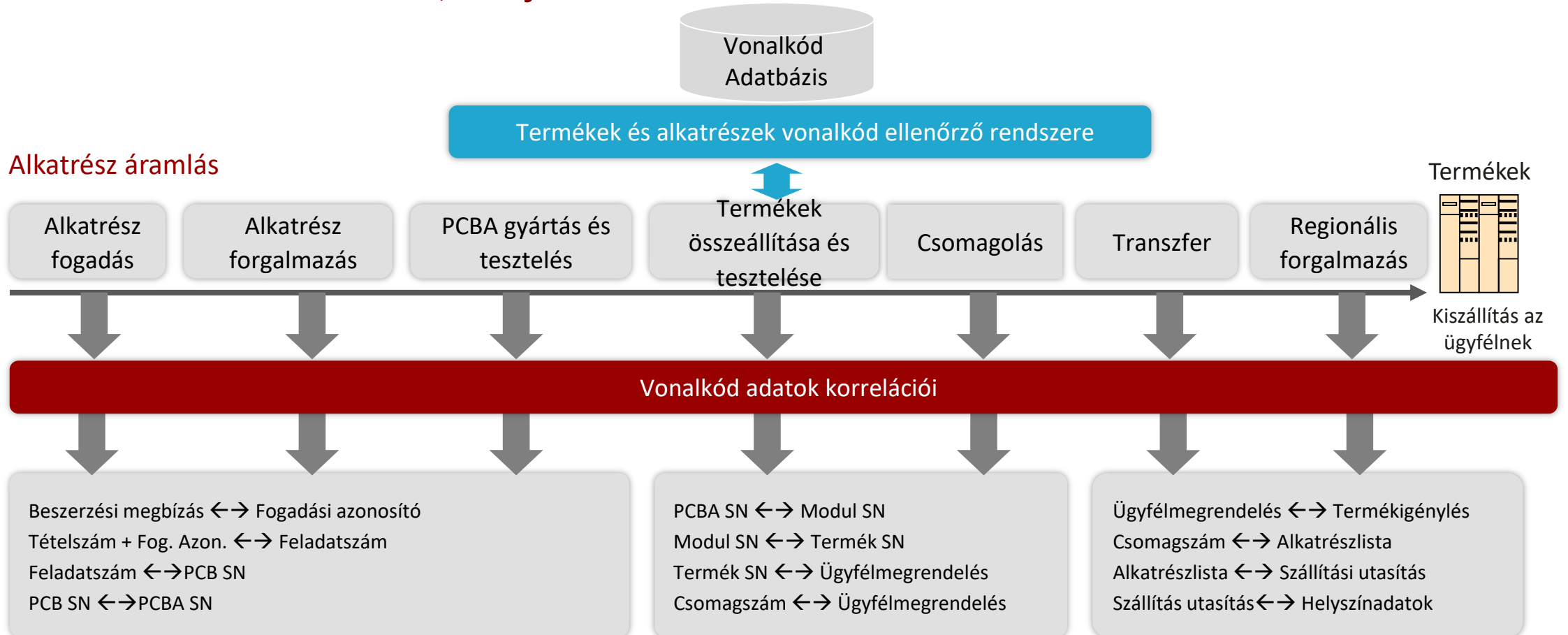


# Szoftverellátási lánc: strukturált információ- és entitáskönyvtárak létrehozása



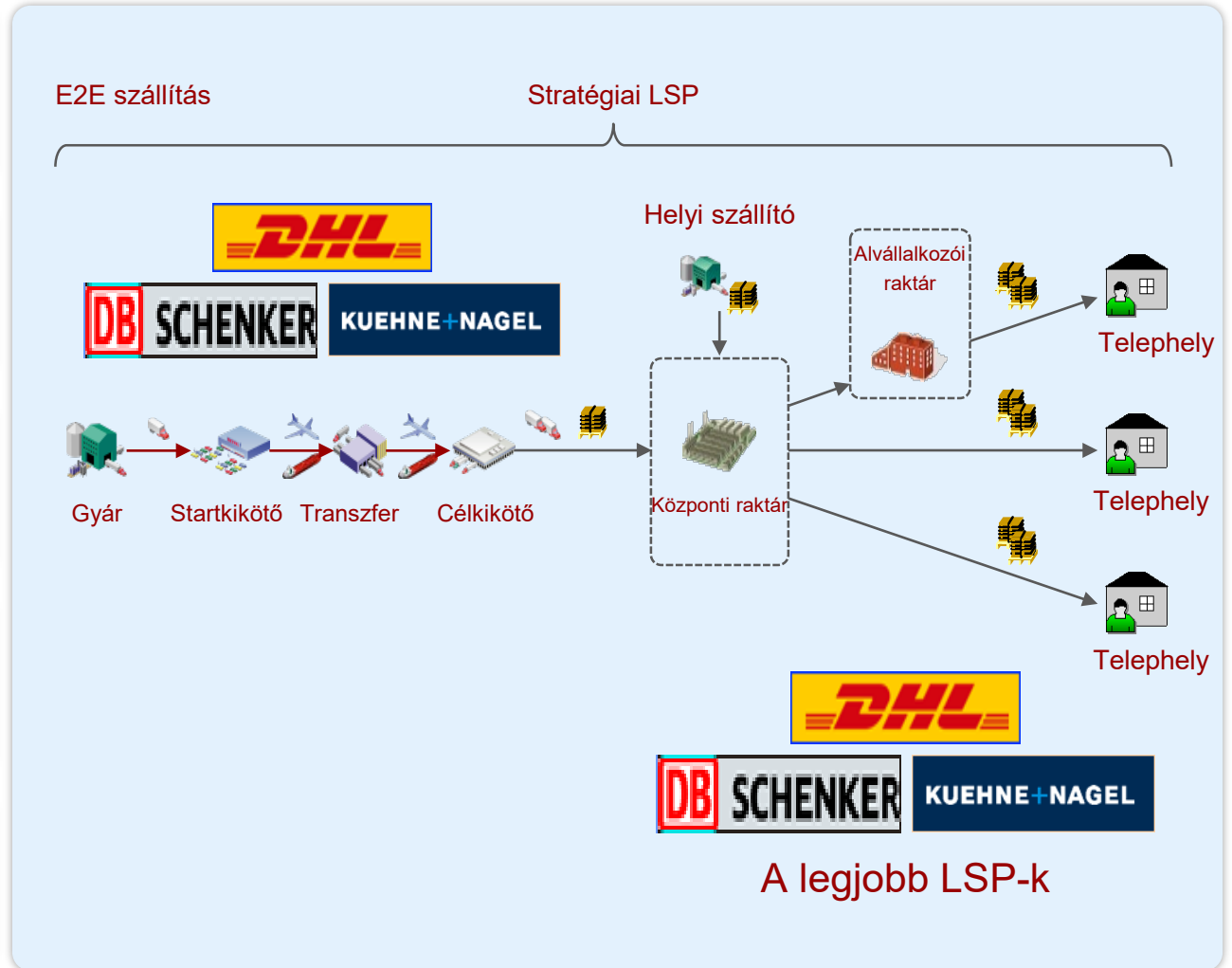
# A végponttól végpontig terjedő nyomonkövethetőségi rendszer lehetővé teszi a gyors problémakezelést

A Huawei 1 órán belül képes azonosítani bármely szoftver, és 4 órán belül bármely hardver életútját (az alkatrészek használatától a vásárlóig). E nyomonkövethetőség támogatása érdekében a Huawei **évente több mint 200 millió vonalkódot használ, amelyek több mint 30 milliárd adatot tartalmaznak.**



# Globális logisztikai menedzsment

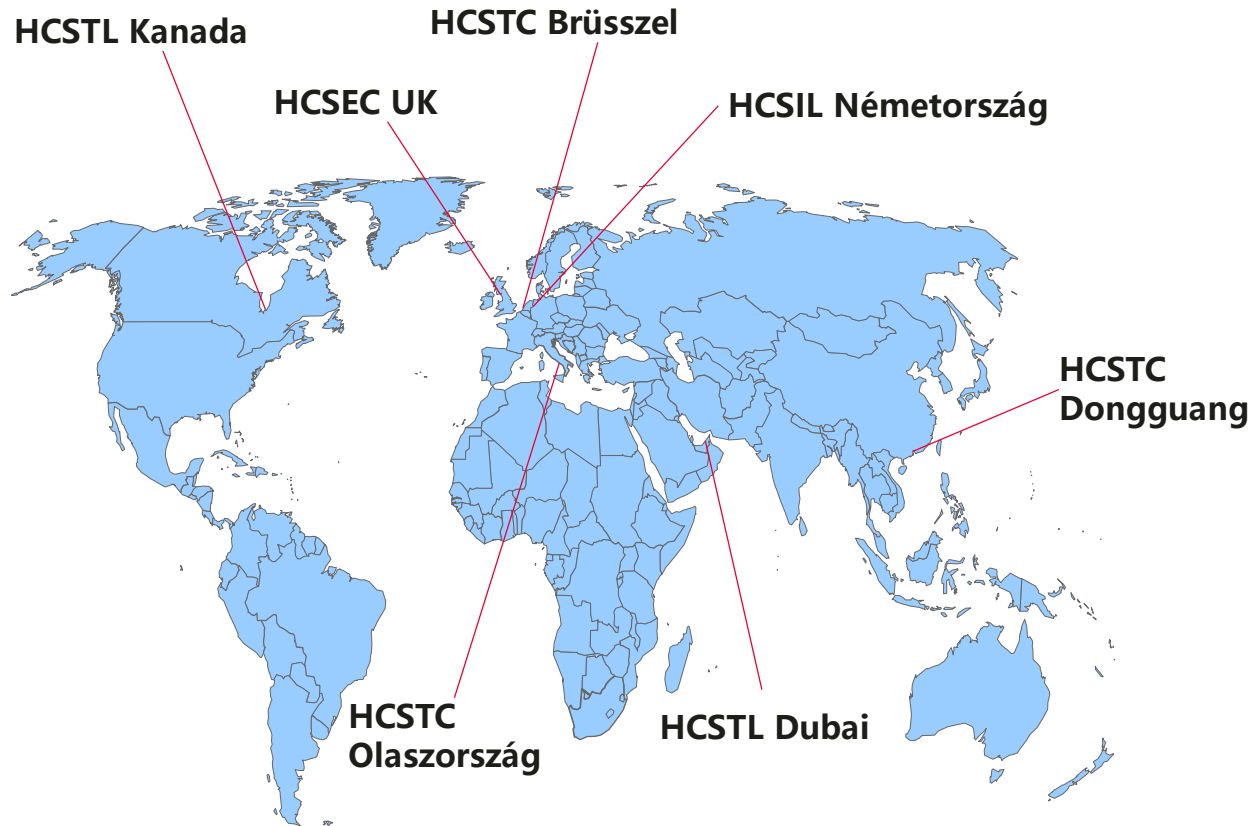
<b>Biztonságos logisztika megoldás</b>	<ul style="list-style-type: none"> <li>• Globális-régió-ország 3 szintű logisztikai megoldás, ISO31000/NIST SP 800-161 szerinti kockázatbecslés minden évben</li> <li>• Az útvonalak biztonsági értékelése félévente</li> <li>• Üzletmenet-folytonosságot biztosító megoldás</li> </ul>
<b>Megbízható LSP</b>	<ul style="list-style-type: none"> <li>• Biztonsági megállapodás aláírása</li> <li>• Minden LSP ISO28000/TAPA/C-TPAT/C-TPAT/AEO/ biztonsági tanúsítvánnyal rendelkezik. NISTIR 7622 stb.</li> </ul>
<b>Vizualizált logisztikai folyamat</b>	<ul style="list-style-type: none"> <li>• Vizualizált szállítási folyamat;</li> <li>• Az informatikai rendszerek rögzítik a logisztikai folyamatok részleteit.</li> <li>• GPS jel 15s-ként egyszer, ha 1 percnél többet nem kapunk, akkor riasztás;</li> <li>• Logisztikai útvonal eltérés riasztás stb.</li> </ul>
<b>Szabványosított raktár menedzsment</b>	<ul style="list-style-type: none"> <li>• C-TPAT/AEO/ISO28000/TAPA követése</li> <li>• Vonalkód rögzítése, amikor a termék elhagyja a raktárat.</li> <li>• 7x24 biztonsági őr és CCTV</li> <li>• Hozzáférés-ellenőrzés</li> </ul>
<b>Visszaru kezelés</b>	<ul style="list-style-type: none"> <li>• Visszaküldött termékek: adattörlesztés</li> <li>• A szabályozások és az ügyfél szabályai és követelményei szerinti kezelés</li> </ul>



# A Huawei globális ellátási hálózata



# Mi is beszállítók vagyunk



**A Huawei átláthatósági központjai lehetővé teszik a teljeskörű ellenőrzést:**

- ✓ Bármilyen szoftver és forráskódra;
- ✓ Az ügyfél vagy harmadik fél által;
- ✓ Bármilyen módszertan és eszköz segítségével;

**7 kiberbiztonsági ellenőrzési projekt:**

- *NCC GROUP (UK),*
- *NIXU (Finnország),*
- *Synopsys (USA),*
- *ERNW (Németország),*
- *SIG (NL).*
- *Tuvit (Németország),*
- *Accenture (Olaszország)*

# ÖSSZEFOGLALÓ

## Ellátási lánc biztonsága

### ALAPELVEK

E2E menedzsment, kiberbiztonság és adatvédelem a tervezésben (Security and Privacy by Design)

### STRATÉGIA

E2E, biztonságos, hatékony, rugalmas

### SZABVÁNYOK

A nemzetközi szabványoknak való megfelelés az ellátási lánc biztonságának érettségéhez vezet



### LESZÁLLÍTÁS

Megbízható gyártás, szoftvermenedzsment, logisztika

### TUDATOSÍTÁS

Fontos, hogy mindenki ismerje a biztonsági szabályokat és az elvárásokat

### NYOMONKÖVETHETŐSÉG

Az ellátási láncban az alkatrészek/termékek minden egyes lépésének, mozgásának nyilvántartása

# Thank you.

Bring digital to every person, home and organization for a fully connected, intelligent world.

**Copyright©2018 Huawei Technologies Co., Ltd.  
All Rights Reserved.**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

