



DIGITAL IDENTITY

ACCESS

GOVERNANCE

CYBERSECURITY

ZERO TRUST

Mario Mínavorský

Zero Trust

ENISA

Zero Trust je bezpečnostný model, v ktorom nie je žiadny používateľ, zariadenie, aplikácia ani sieť dôveryhodná „predvolene“ — ani keď je vo vnútri firemného perimetra; prístup sa povoľuje až po overení.

NIST

NIST opisuje Zero Trust (ZT) ako prístup, ktorý presúva obranu zo statického „sieťového perimetra“ na používateľov, zariadenia a chránené zdroje.



Identita je nový perimeter

- Bezpečnosť sa dnes nerozhoduje na hranici siete.
- Rozhoduje sa v momente, keď niekomu povoľujeme prístup.
- Identita nahrádza sieť ako hlavný riadiaci bod.





Business

Hybridná práca a cloud zrušili jednotnú hranicu.

Musíme prijať, že „vnútri siete“ už neznamená bezpečne

Schváliť model prístupu pre hybrid

IT / Service

Používatelia, aplikácie a dáta sú roztrúsené.
Model „vnútri = bezpečné“ už neplatí.

Inventarizovať kritické systémy a prístupy

Zaviesť jednotné logovanie a viditeľnosť

Perimeter sa rozpadol

Zero Trust – princíp

- Zero Trust nie je produkt ani architektúra.
- Je to princíp rozhodovania o prístupe.
- Overujeme identitu, kontext a riziko pri každom prístupe.





Business

Definovať roly, zodpovednosti a vlastníkov prístupov

Trvať na tom, že zmena role = zmena prístupu

IT / Service

Spravovať oprávnenia (kto/čo/prečo) a pravidelné revízie

Zaviesť dohľadateľnú stopu pre kritické prístupy

Identita rozhoduje

Prečo je to tak?

01

Hybridná realita

- Väčšina organizácií má viacero identít a systémov.
- Problém nie je ich počet.
- Problém je nejednotné riadenie prístupu.

02

Prístup

- Každý prístup je rozhodnutie.
- Kto žiada, ku čomu, za akých podmienok.
- Rozhodnutie musí byť konzistentné a dohľadateľné.

03

Pravidlá

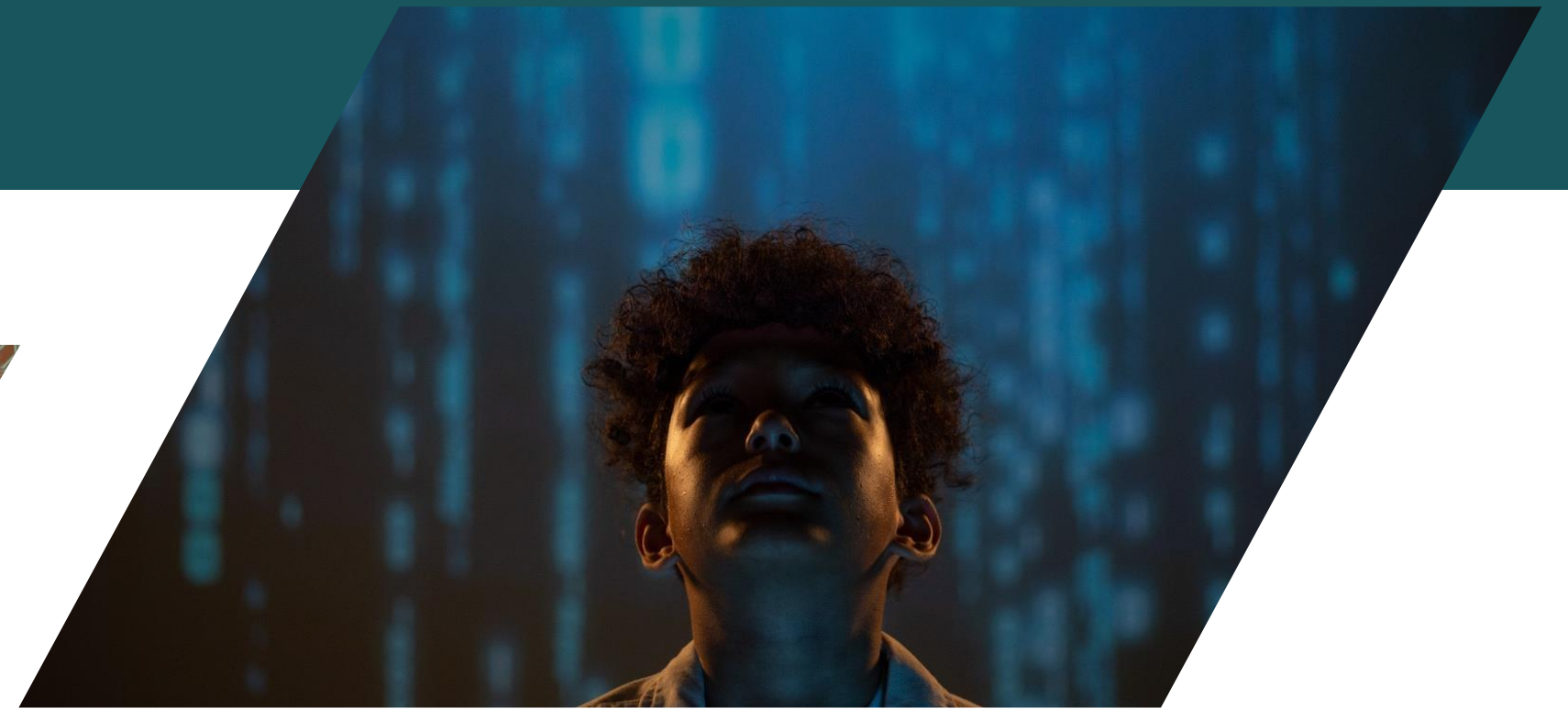
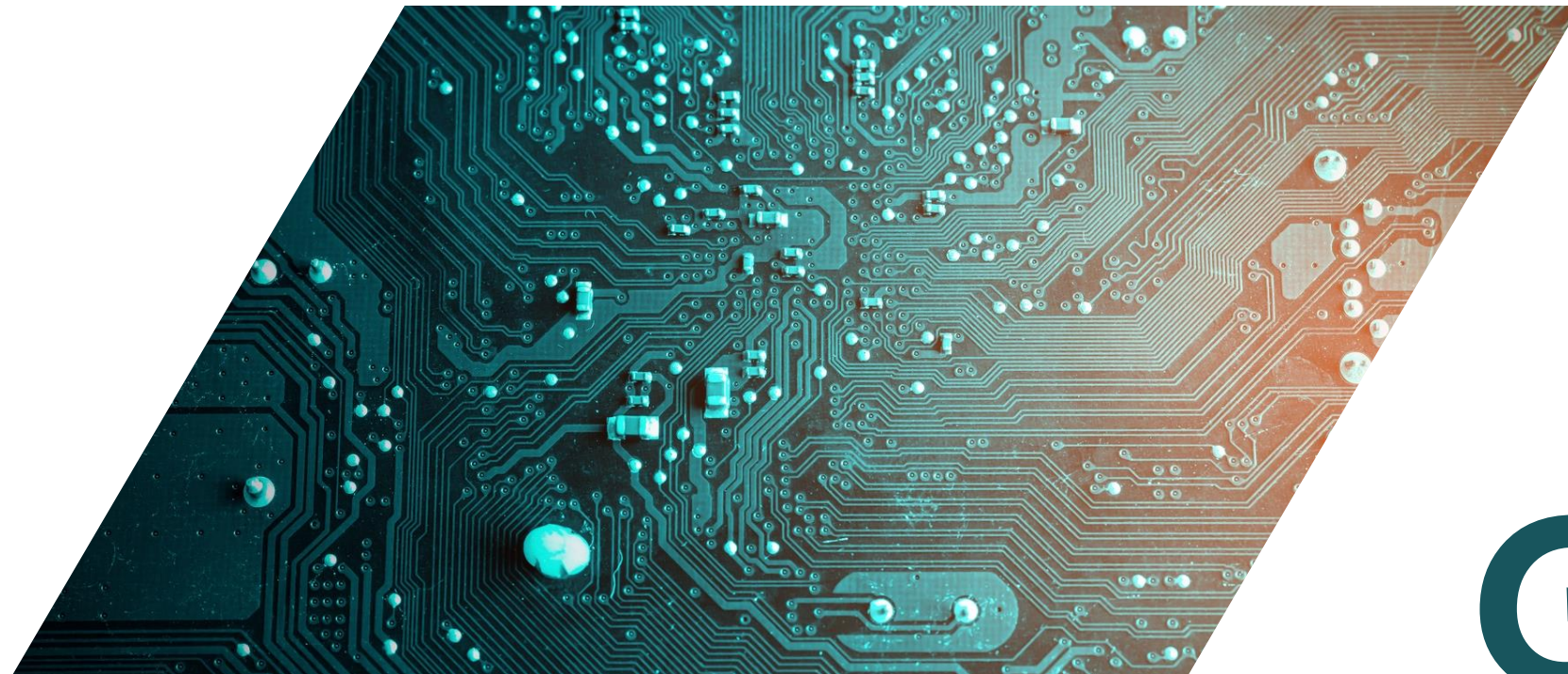
- Pravidlá definujú hranice zodpovednosti.
- Nie IT dokument, ale rozhodnutie vedenia.
- IT – technická realizácia.



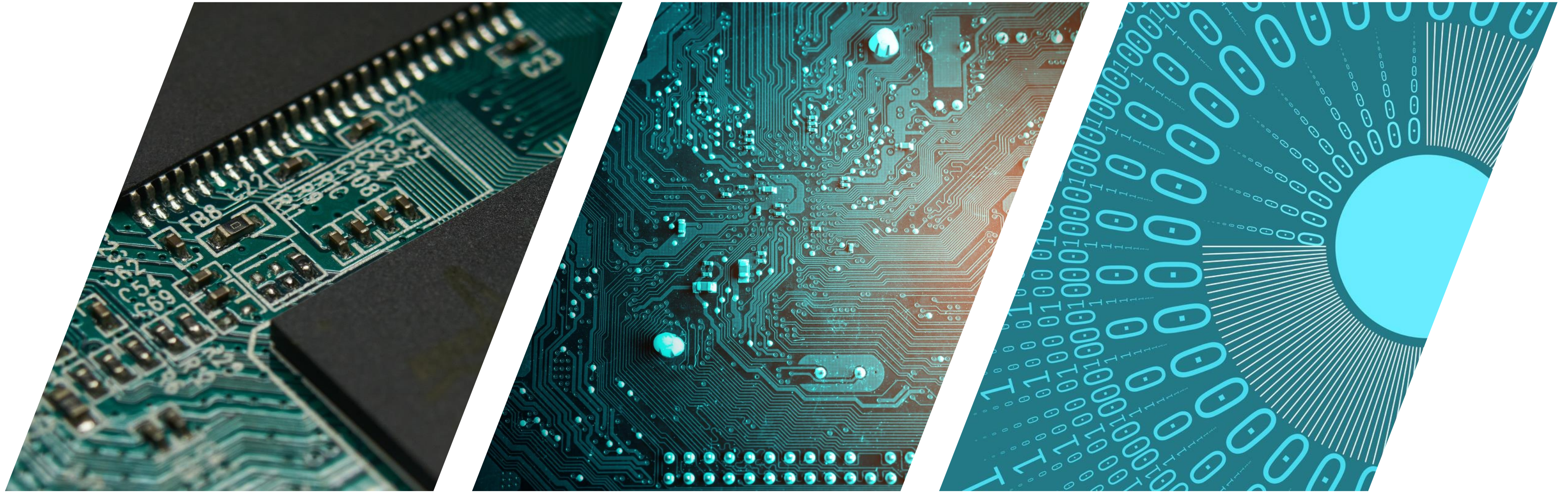
- Administrátori – najvyššia koncentrácia právomocí.
- Financie – priamy finančný dopad.
- Externisti – slabá kontrola a dohľad.

- Výnimky sú nevyhnutné, ale nebezpečné.
- Bez vlastníka a expirácie rastie riziko.
- Riadené výnimky zvyšujú odolnosť.

- Prístupy musia kopírovať pracovný život.
- Nástup, zmena, odchod.
- Oneskorenia znamenajú riziko.



GOVERNANCE



??? Q / A ???



Dovidenia.



Email

info@credibilis.sk



THANK YOU

Cybe Bard Talks

