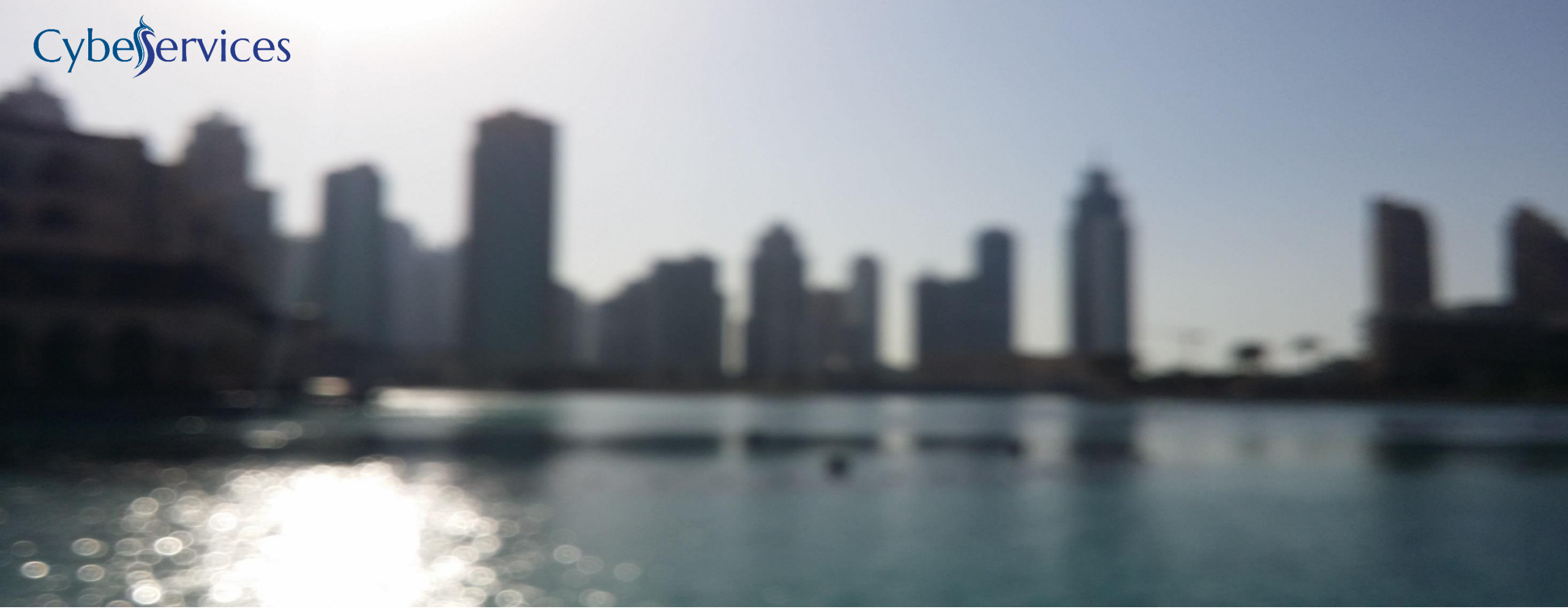
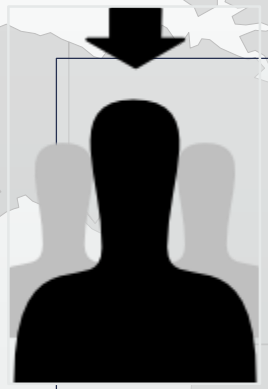


Az IT biztonság üzleti vetülete, avagy kiberbiztonság 2017-2021

Mádi-Nátor Anett, vezérigazgató h., stratégiai üzletfejlesztés
Cyber Services Zrt.

Globális változások



7 milliárd Internet felhasználó 2020-ra

55-200 milliárd összekapcsolt eszköz

Internet of things

Globális szakemberhiány

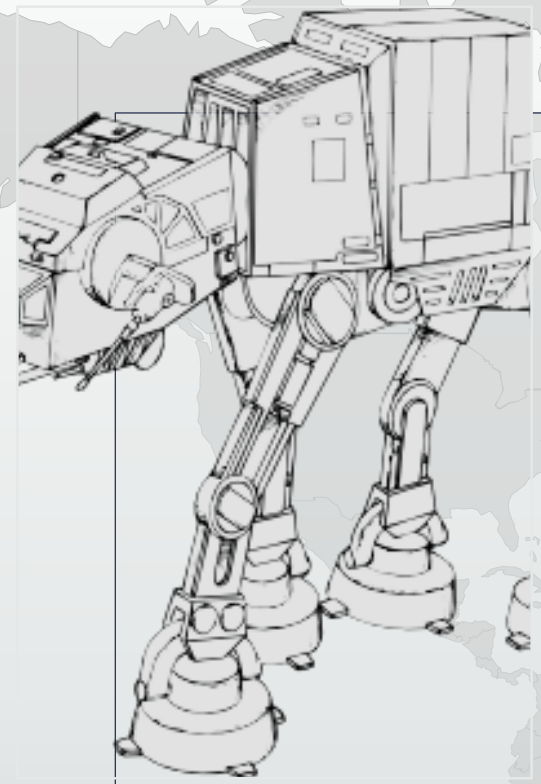
Ami látható

Kiberbiztonsági mutatók 2017-2021

A kibervédelmi szakértők $6000 milliárd veszteséget jósolnak 2021-re.

Ami sejthető

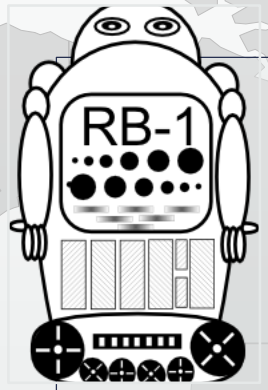
Kiberbiztonsági mutatók 2017-2021



5. hadszíntér

Ami már valóság

Globális változások 2016-2017

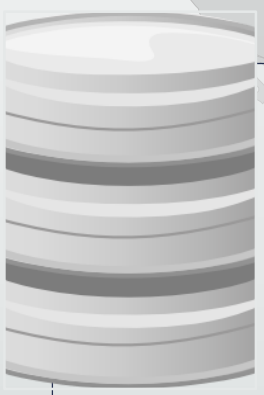


#Botnet fertőzöttség

Magyarország

EU 1., EMEA 3.

#Zsarolóvírusok 727% globális növekedés



#Adatszivárgás átlag 74.000.000/hó (globális átlag)

#APT 400% globális növekedés

Amit érteni kell

Globális változások 2016-2021

Digitalizáció

- Ipar 4.0
- Felhősödés
- Értéklánc digitalizációja
- Fogyasztás alapú modell
- A CEO-k 30% elbukik – előrejelzés 2021-re
- A cégek 70% eltűnik – előrejelzés 2021-re

Amire készülni kell

Globális változások 2016-2021

A legkeresettebb szakértők a jövőben

- Data scientists
- CX professionals
- Experience designers
- Digital business leaders
- Software developers
- Analysts skilled at statistical and predictive analytics
- Consultant sellers
- Cybersecurity professionals
- Content professionals skilled at storytelling
- Augmented and virtual reality designers

Amire készülni kell

Globális változások 2016-2021

Fenyegetések 2017-2019

- Hálózati kapcsolódást ellehetetlenítő támadások (Brazil bank, 2016. október)
- Zsarolóvírusok az IoT ellen (Wannacry, 2017)
- Privileged insiders – kiemelt felhasználók, vezetők elleni célzott támadások
- Hamis adatintegritás (SWIFT, 2016-folyamatban)
- Automatizált dezinformáció – adatvezérelt szakújságírás (USA elnökválasztás, 2016)
- Információ torzítás (GPS jeltorzítás, Dél-Korea, 2012, 2016, 2017)
- Blockchain sérülékenységek – mert az infrastruktúra hagyományos (2013-folyamatban)
- Nemzetbiztonsági érdekek a magán/üzleti érdekekkel szemben
- AI alapú támadások – automatikusan támadó botnetek (Github, open source eszköz elérhető)

Amit kezelni kell

Kibertámadások – személyes

Fenyegetések 2017-2019

- Levelezés
- Közösségi profilok
- Banki információk
- Zsaroló vírusok
- Digitális nyomkövetés
- Profil hamisítás
- Reputációt érintő támadások
- Nemzetbiztonsági érdek a magánérdek ellen

Amit kezelni kell

Kibertámadások – céges

Fenyegetések 2017-2019

- Vállalati levelezés
- Zsarolóvírusok
- Reputáció alapú támadások
- Hamisított weboldalak
- Hamisított emailek
- Deface (tartalommódosításos támadás)
- Adatlopások
- Botnet
- Belső fenyegetés (insider threat)
- Humán oldali támadások, pszichológiai manipulációs támadások (social engineering)
- Nemzetbiztonsági érdekek az üzleti érdekekkel szemben

Amit kezelni kell

CyberServices

Business values - impact

CEOs will exit 30% of their CMOs for not mustering the blended skill set of design and analytics.

In 2017, CIOs will take the plunge and become business leaders to address external and personal risk.

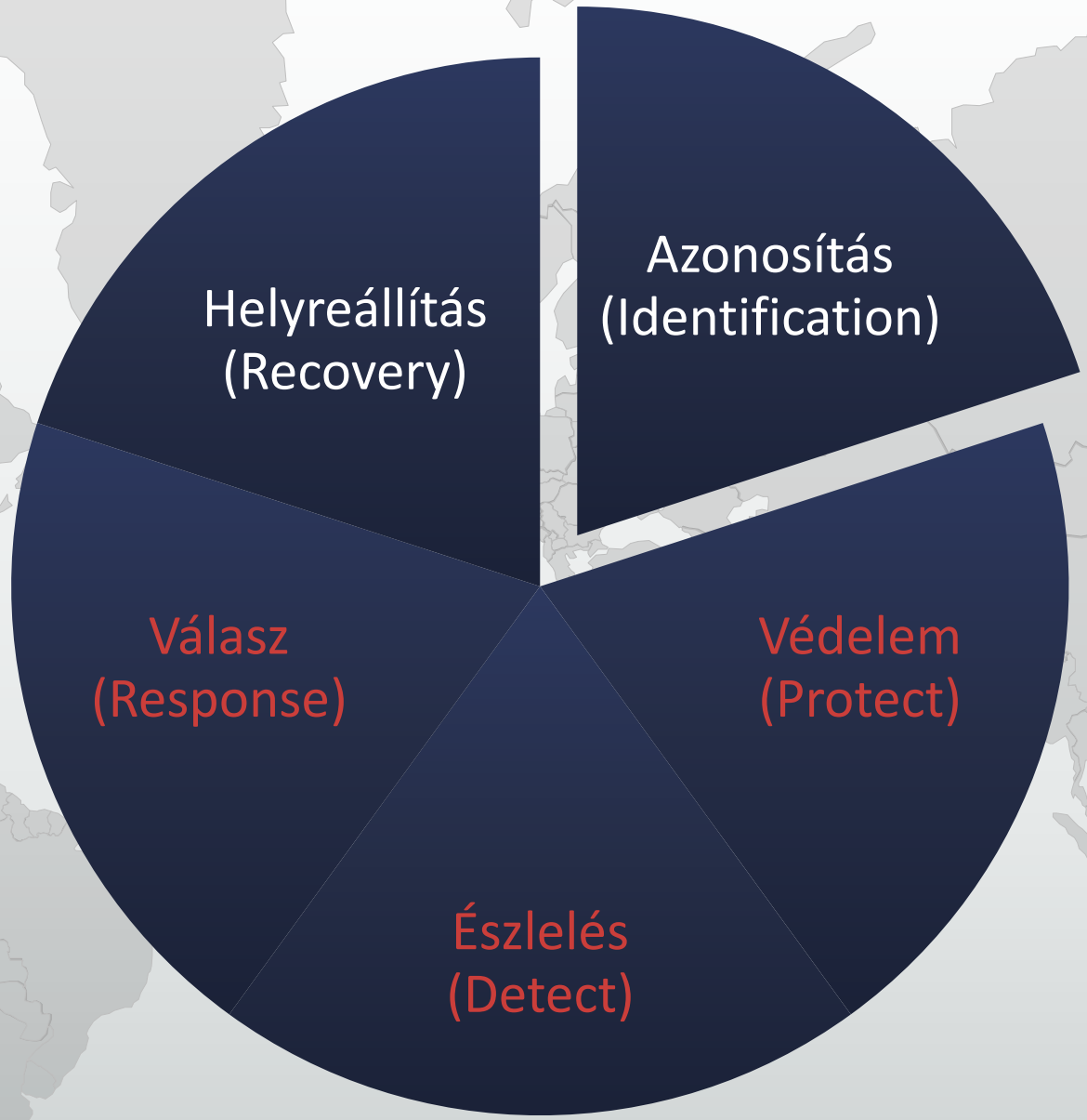
Business heads will see doubled attrition rates as CEOs dig in and appoint leaders with both digital and customer competencies.

Transitional roles like chief data officer, chief digital officer, and chief customer officer will continue to get reintegrated into traditional roles.

In 2017, the basic fabric of trust is at stake as CEOs grapple with how to defend against escalating, dynamic security and privacy risk.

Source: FORRESTER.COM

Hiányzó kiberbiztonsági képességek (fehérrel)



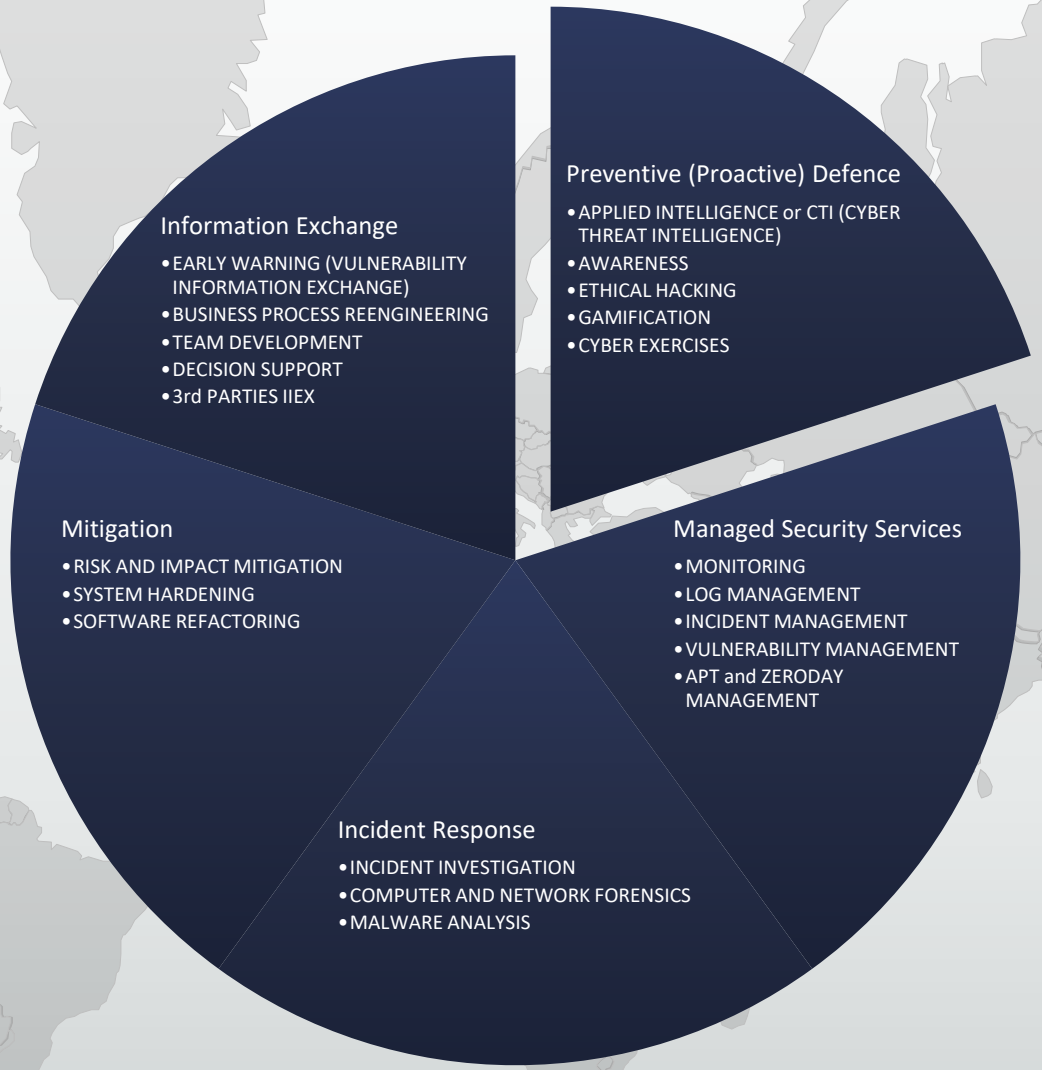
NIST-800-53

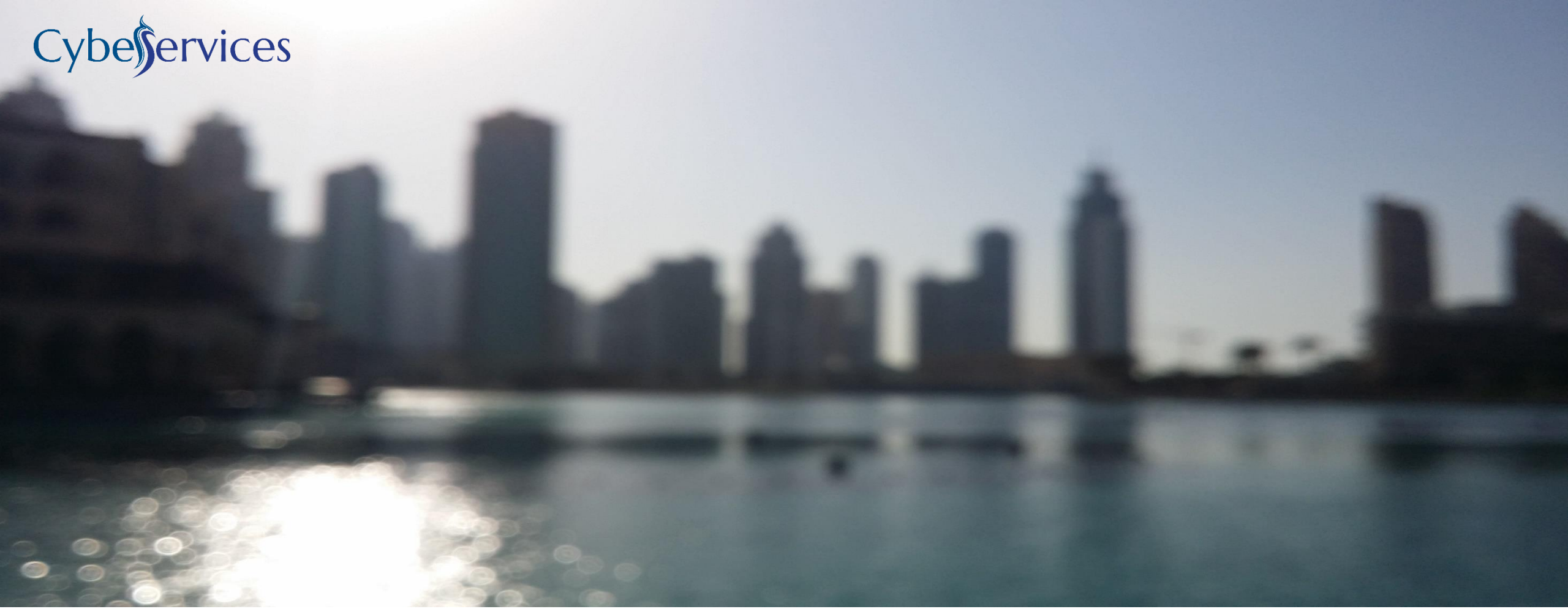
A válasz – kiberbiztonsági képességek fejlesztése

- Biztonsági kontrollok, technikai és adminisztratív képességfejlesztés – NIST, GDPR, NIS
- Képességfejlesztő kibergyakorlatok – új képességek kialakítására
- Folyamatvalidáló kibergyakorlatok – meglévő folyamatok működőképességének ellenőrzésére
- Kiberbiztonsági tudatosító kampányok
- Információmegosztás
- Kiberbiztonsági döntés- és döntéstámogató képesség kialakítása

NIST-800-53

Kiberbiztonsági portfolió





Köszönöm a figyelmet