secudit the risk analyzer

DUNAÚJVÁROSI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME

Elosztott fenyegetettség felmérés

Dr. Leitold Ferenc
Dunaújvárosi Egyetem, Secudit Kft.

Hadarics Kálmán
Dunaújvárosi Egyetem

Tartalom

secudit the risk analyzer

- Bevezető gondolatok
- A modell felépítése
- Belső szenzorok
- Külső szenzorok
- Elosztott veszélyeztetettségi metrika
- Felhasználói biztonságtudatosság automatikus figyelése
- Adatbiztonsági kérdések a GDPR tükrében

secudit the risk analyzer

Bevezető gondolatok

Apple watch saved Alberta man's life, makes international headlines

'I bought the watch two weeks before the heart attack, so it was the right time'

By Wallis Snowdon, CBC News · Posted: Mar 17, 2016 8:21 AM MT | Last Updated: Mar 17, 2016 1:22 PM MT

Dennis Anselmo, a watch fanatic, shows off his life-saving Apple watch. (CBC)

Listen

Smart watch alerts user to impending heart attack 5:36

A Morinville, Alta., contractor who says his life was saved by a smartwatch, is making headlines the world over.

Dennis Anselmo says the high-tech gadget warned him of an impending heart attack.

Now, six months since he was released from hospital, dozens of news outlets, including **The Sun** and **The Daily Mirror** in Great Britain, have picked up his story as an example of the merits of wearable technology

Weather

CBCnews | Edmonton

LIVE Edmonton More Streams
Radio One
Listen Live

Home | Opinion | World | Canada | Politics | Business | Health | Entertainment | Technology & Science | Video

Canada | Edmonton

secudit the risk analyzer

Apple watch saved Alberta man's life, makes inte headlines

'I bought the watch two weeks before the heart attack, so it was the right time'

By Idella Shewish, CBC News · Posted: Mar 17, 2016 8:21 AM MT | Last Updated: Mar 17, 2016 1:22 PM MT

Dennis Anselmo, a watch fanatic, shows off his life-saving Apple watch. (CBC)

Listen

Smart watch alerts user to impending heart attack 5:36

1198 shares

Facebook

A Morinville, Alta., contractor who says his life was saved by a smartwatch, is making headlines the world over.

Dennis Anselmo says the high-tech gadget warned him of an impending heart attack.

Now, six months since he was released from hospital, dozens of news outlets, including **The Sun** and **The Daily Mirror** in Great Britain, have picked up his story as an example of the merits of wearable technology

Stay Connected

Mobile | Facebook | PC

Szívinfarktustól mentett meg egy embert az Apple Watch

Weather

Wednesday | Thursday | Sunday

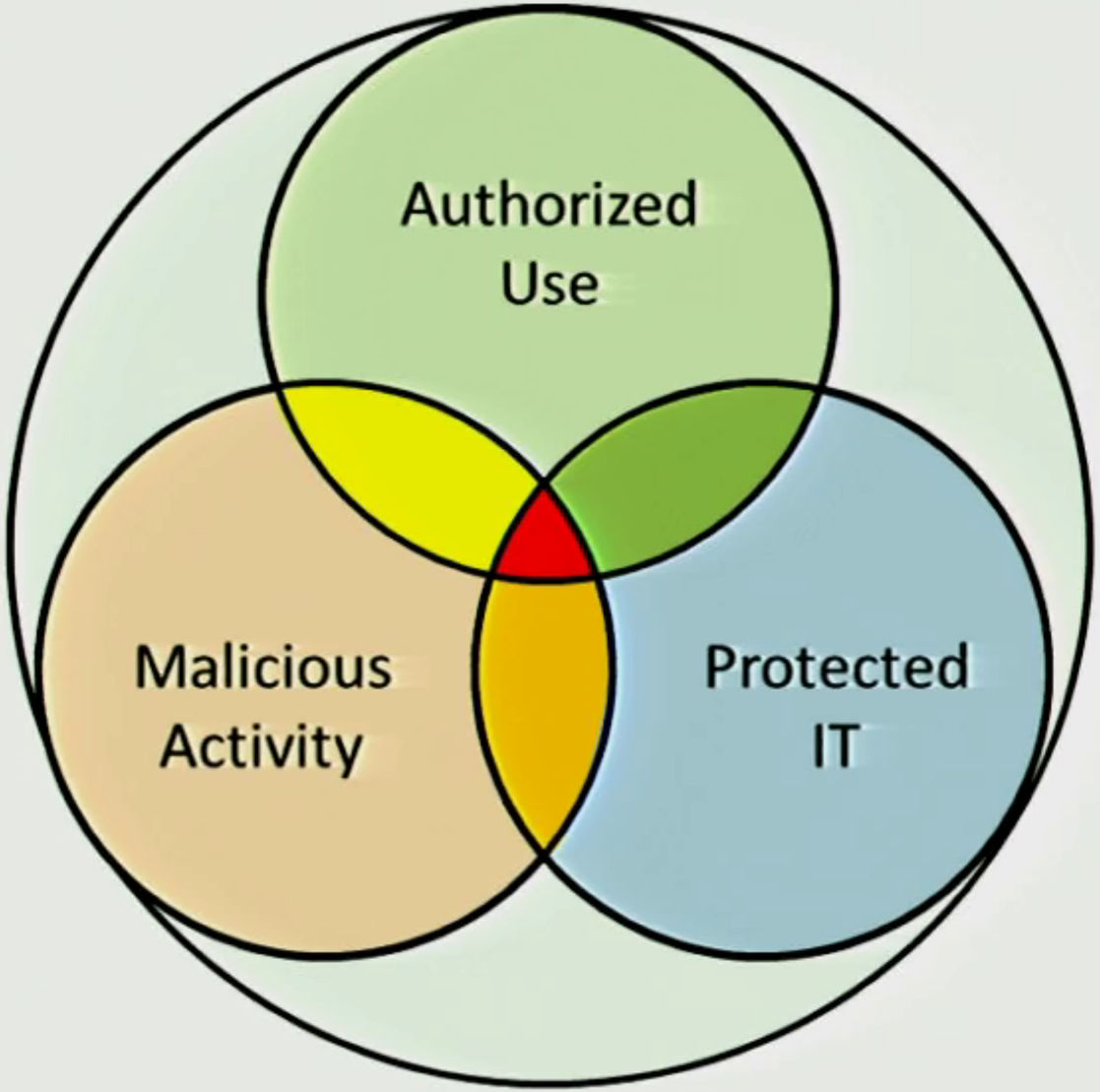
1°C | -2°C

Rátfai Gábor
ÚJSÁGÍRÓ 2016. 03. 16. 10:00

Egy okosórán múlott a kerítésépítő férfi élete: úgy tűnik, az okos kütyük néha sokkal többet is tudnak, mint amire tervezték őket.

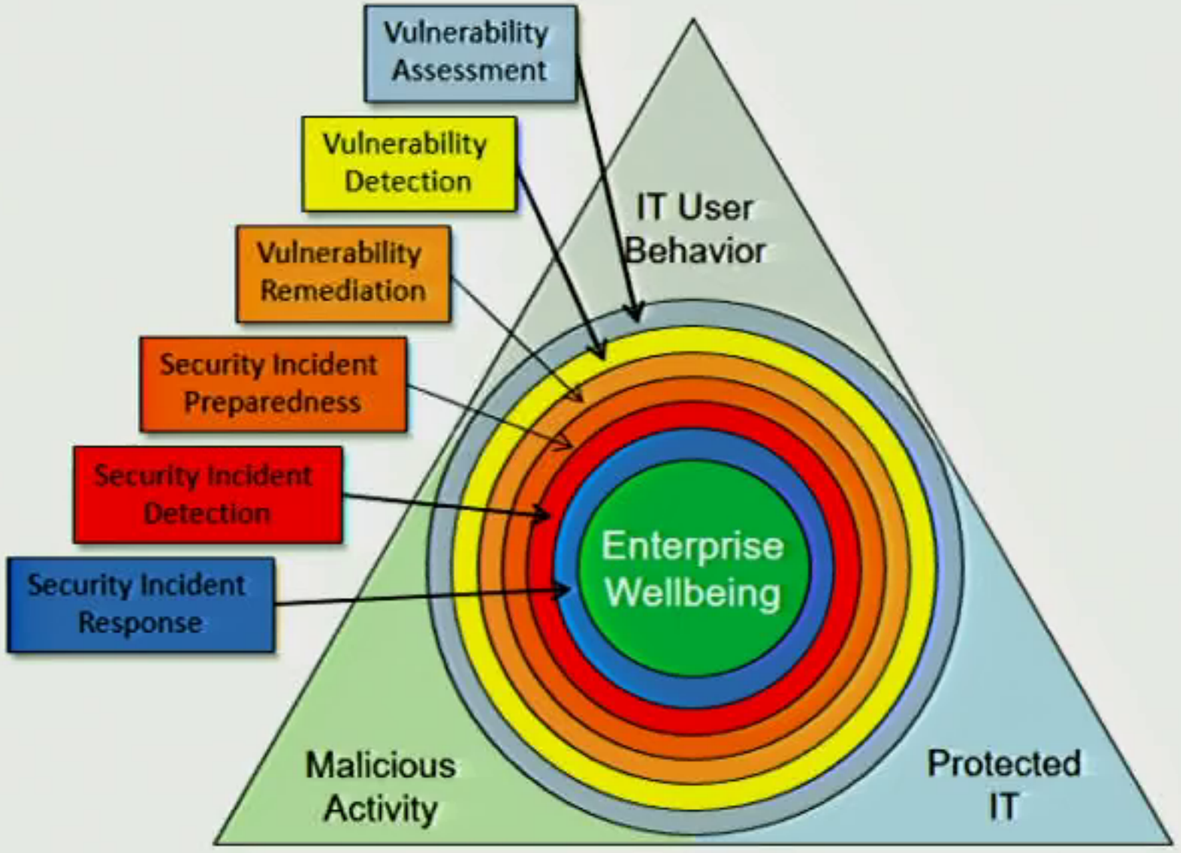
Distributed Vulnerability Assessment

secudit the risk analyzer



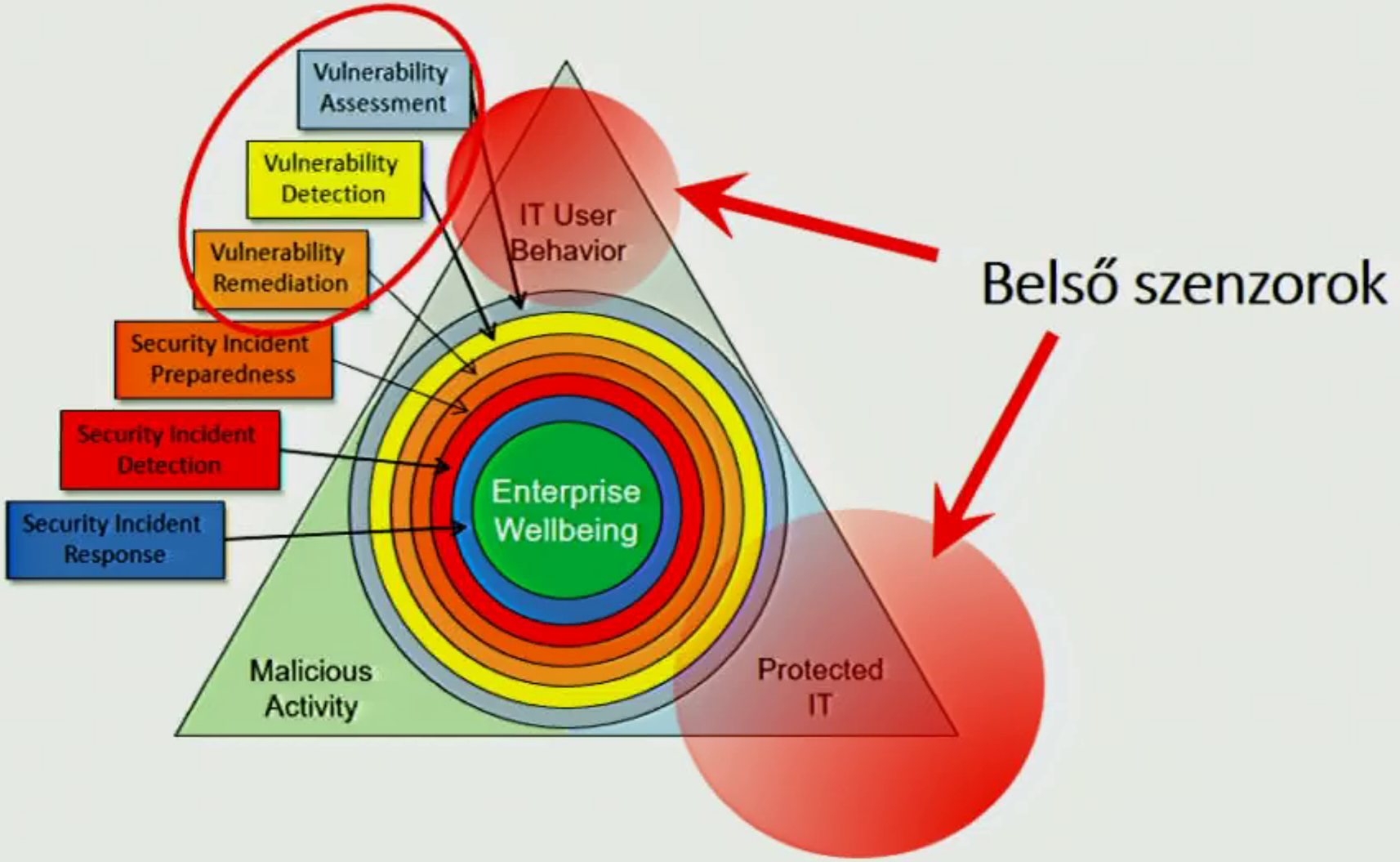
Distributed Vulnerability Assessment

secudit the risk analyzer



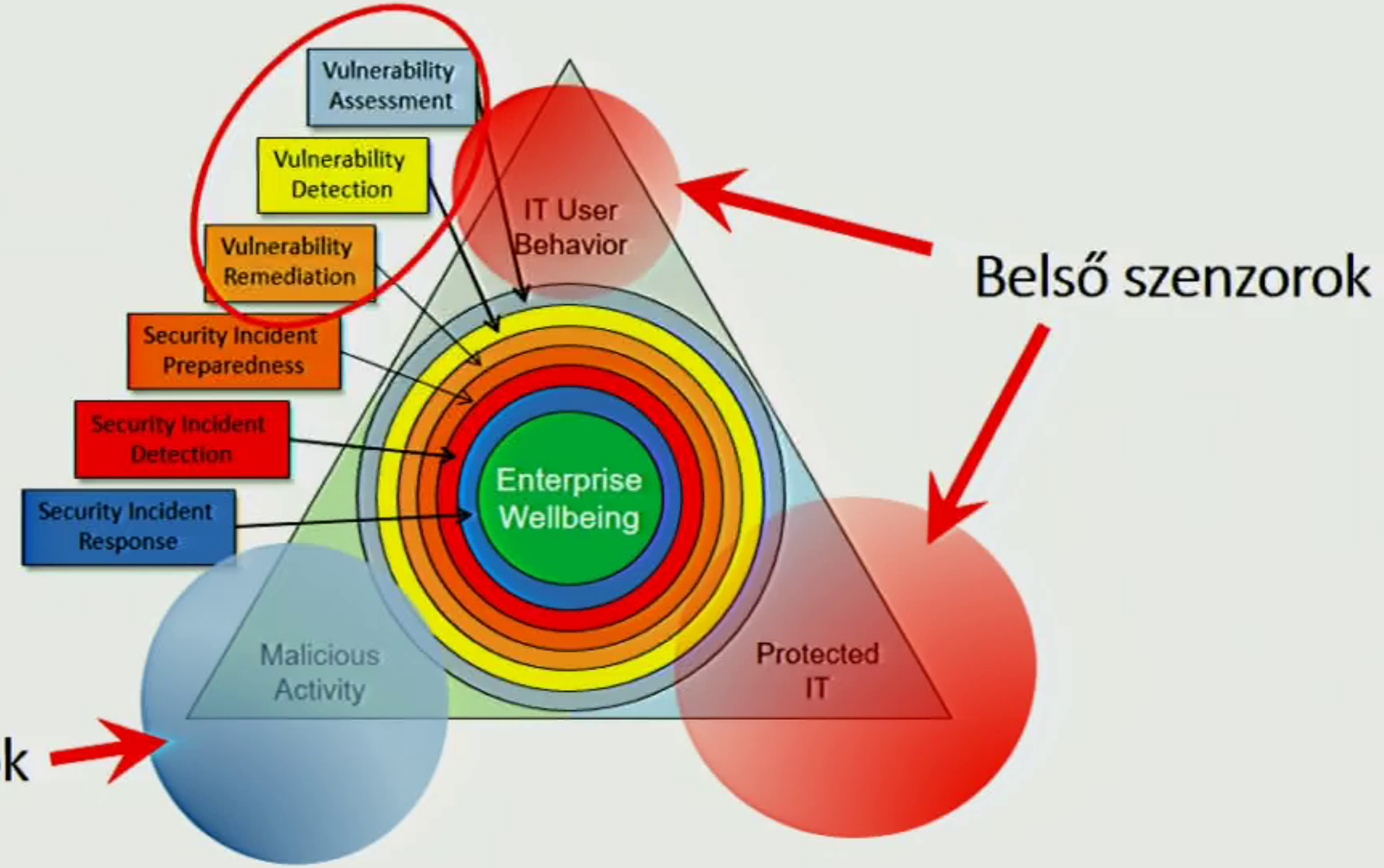
Distributed Vulnerability Assessment

secudit the risk analyzer



Distributed Vulnerability Assessment

secudit the risk analyzer



Belső szenzorok

Külső szenzorok

secudit the risk analyzer

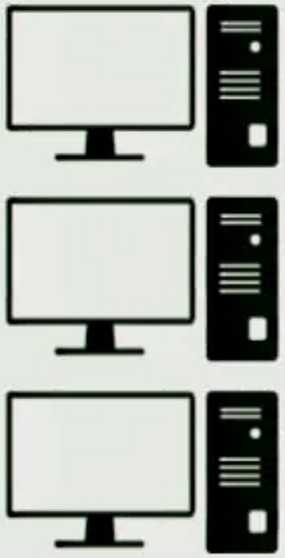
A modell felépítése

A modell felépítése

secudit the risk analyzer

Külső szenzorok, előzetes vizsgálatok

Belső szenzorok



Számítások

Veszélyeztetettségi metrika

secudit the risk analyzer

Belső szenzorok

Változások követése

secudit the risk analyzer

Fontos, hogy a gyűjtött információ
mindig az aktuális állapotot tükrözze

Változások követése

secudit the risk analyzer

Fontos, hogy a gyűjtött információ
mindig az aktuális állapotot tükrözze

Automatizálás

Összegyűjtött adatok

secudit the risk analyzer

- Hardware információk
- Sensor adatok
- Telepített szoftverek
- Telepített OS frissítések
- Hálózati interface-ek monitorozása
- Folyamatok elindulása/leállása
- Szolgáltatások
- Registry, WMI adatok
- Böngészés monitorozása

secudit the risk analyzer

Külső szenzorok

Vizsgálathoz szükséges információk

secudit the risk analyzer

- Informatikai fenyegetések információi
- Hardware információk
- Felhasználói viselkedésinformációk

Veszélyforrásokra vonatkozó információk

secudit the risk analyzer

- Kompatibilitás
  - Operációs rendszer
  - Böngésző
  - Egyéb telepített alkalmazás
- Védelem blokkolási képessége
- Elterjedtség
- Szükséges felhasználói interaktivitás

Információk gyűjtése

secudit the risk analyzer

- Sandbox környezet
  - Automatizált környezet
  - Részletes elemzés
  - Antivírus és kompatibilitás vizsgálat
- Harmadik féltől származó információk
  - NSSLabs CAWS szolgáltatása
  - AV tesztelők
  - Védelmi rendszerek gyártói

KEEP CALM AND COLLECT THEM ALL

secudit the risk analyzer

Elosztott veszélyeztetettségi metrika

Matematikai háttér

secudit the risk analyzer

$$p_s(l) = 1 - \prod_{for\ all\ t,u\ and\ i} (1 - p_{user}(t,u) \cdot p_{device}(t,i) \cdot p_{prev}(t,l))^{k(t,u)}$$

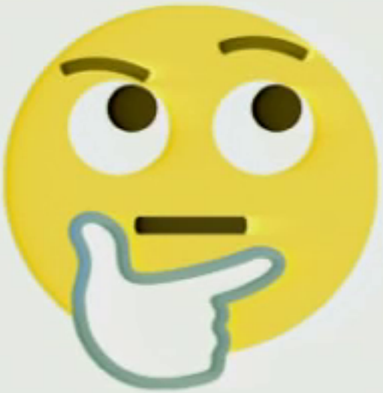
K. Hadarics, K. Győrffy, B. Nagy, L. Bognár, A. Arrott, F. Leitold:
Mathematical Model of Distributed Vulnerability Assessment
9th International Scientific Conference, Security and Protection of Information, 2017, Brno, Czech Republic

F. Leitold , A. Arrott, K. Hadarics:
Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility
24th Annual EICAR Conference, Nuremberg, Germany, 2016

Mi lenne, ha?

secudit the risk analyzer

- Változtatható:
  - Operációs rendszer
  - Böngésző
  - Védelem
- Törölhető/Telepíthető alkalmazások
- Felhasználó oktatása



secudit the risk analyzer

Felhasználói biztonságtudatosság automatikus figyelése

Mit mérjünk?

secudit the risk analyzer

- Eszközök használata
- Alkalmazások használata
- Kommunikációt biztosító alkalmazások használata
- Állományok megnyitása, továbbküldése
- Védelmi rendszerek kezelése (pl.: frissítés, tiltás)
- Interneten történő böngészés
- …

Hogyan mérjünk?

secudit the risk analyzer

Szokásos használat megfigyelése

PASSZÍV MÓDSZER

Felhasználói interaktivitás kiváltása, válasz megfigyelése

AKTÍV MÓDSZER

secudit the risk analyzer

Adatbiztonsági kérdések a GDPR tükrében

Felhasználói biztonságtudatosság mérése vs. GDPR

secudit the risk analyzer

Analógia

secudit the risk analyzer

Hogyan legyen a felhasználói biztonságtudatosság felmérése GDPR kompatibilis?

secudit the risk analyzer

Rengeteg papírmunka

- érdekegyeztetés
- hatástanulmány
- tájékoztatás

→ szabályozás segítése

A személyes adatok használatának korlátozása

- pl. fájlok tárolása helyett hash-ek, tag-ek használata
- időbeli korlátozás
- személyes adatok esetleges vizsgálata az érintett jelenlétében

secudit the risk analyzer

Az egyik legfontosabb, felhasználói viselkedésre utaló mérés arra vonatkozik, hogy egy felhasználó mit kezd egy email-ben kapott melléklettel …

Két információforrás:

- email mellékletek
- elindított alkalmazások, megnyitott file-ok

A cél érdekében nem szükséges a mellékletet eltárolni, elég a melléklet hash értéke.

www.secudit.com

secudit the risk analyzer

DUNAÚJVÁROSI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME