Elosztott fenyegetettségi felmérés

Dr. Leitold Ferenc
ügyvezető, Secudit Kft.

Információvédelem menedzselése LXXXI. Szakmai fórum
Hétpecsét Információbiztonsági Egyesület
2018. május 16.

CBCnews | Edmonton

LIVE Edmonton More Streams
Radio One
Listen Live

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

Canada > Edmonton

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 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

1198 shares

Facebook

Stay Connected

Mobile Facebook

Weather

Wednesday Thursday Sunday

1°C -2°C

secudit the risk analyzer

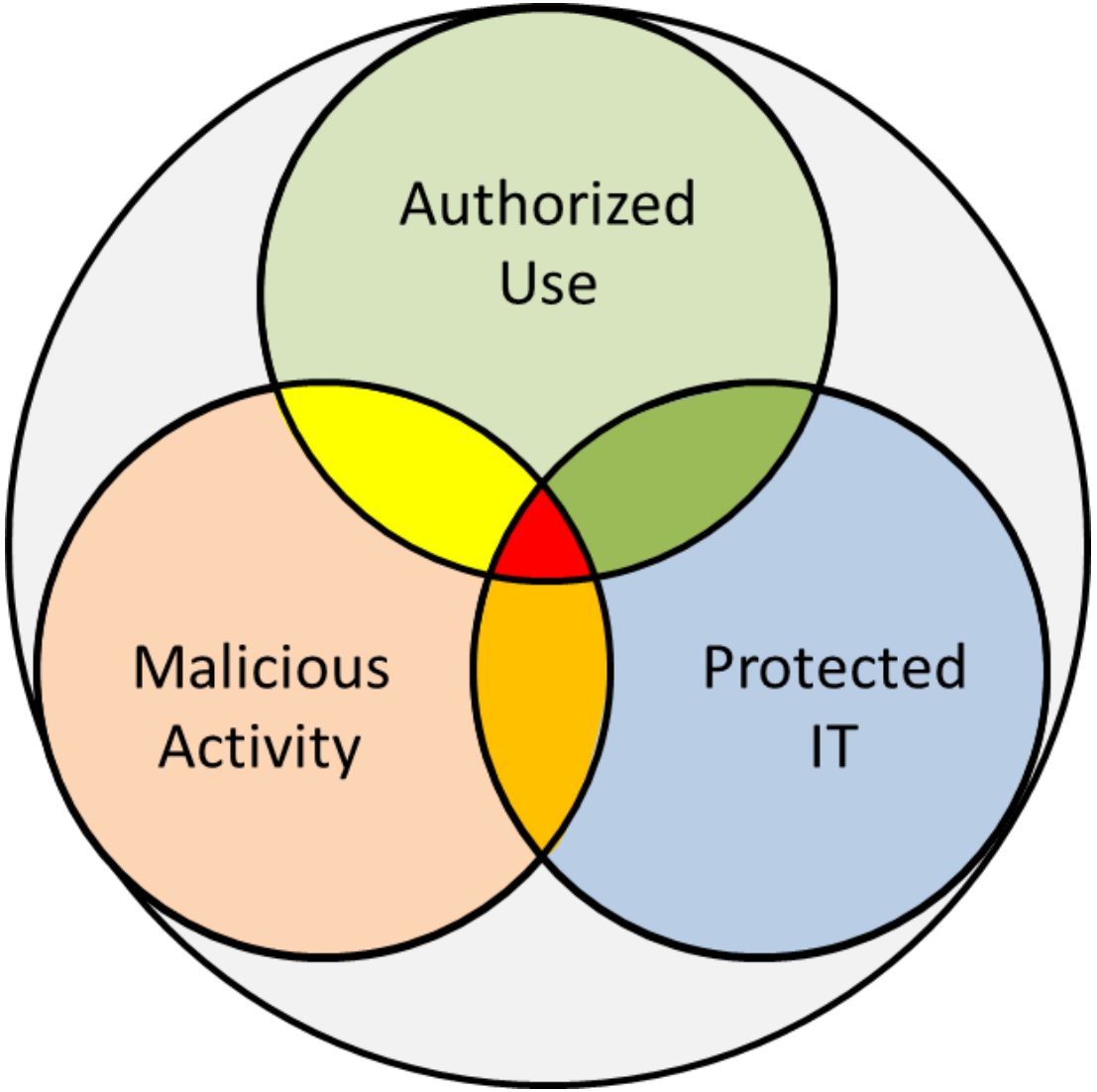
Szívinfarktustól mentett meg egy embert az Apple Watch

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.

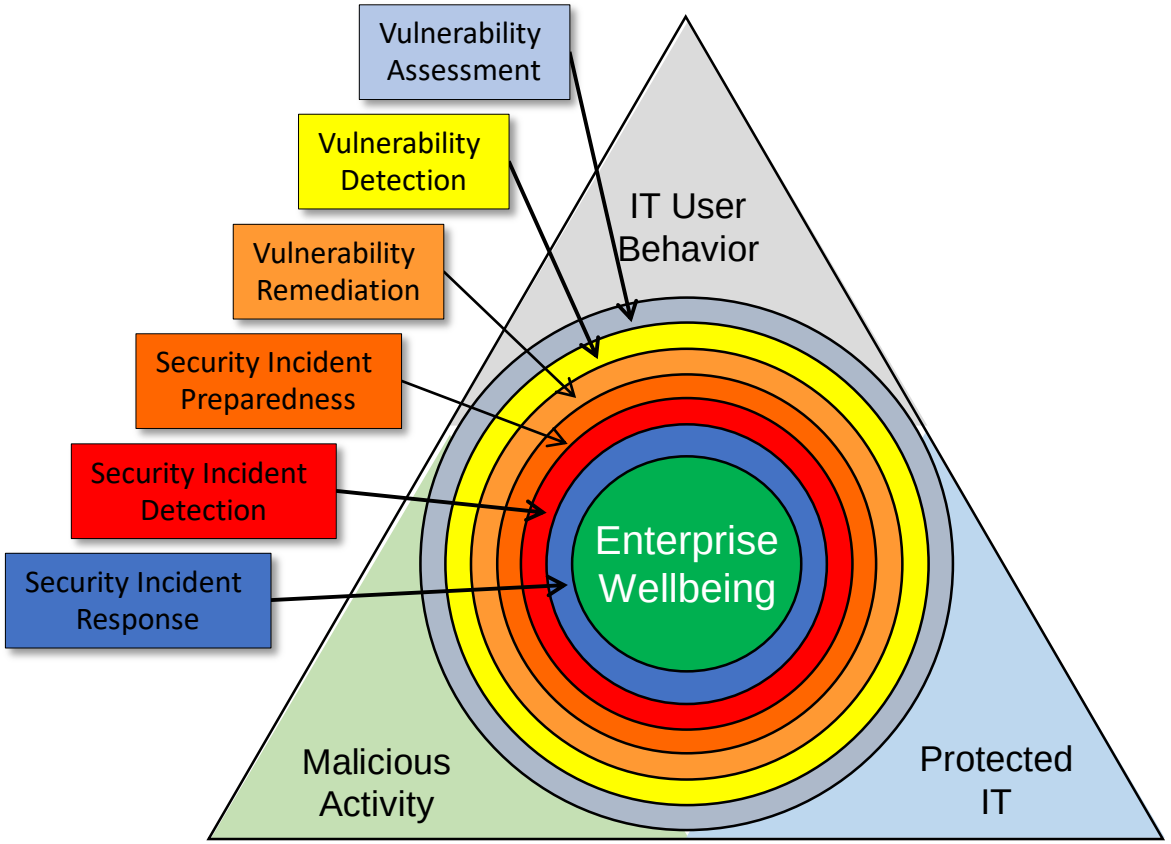
DVA - Distributed Vulnerability Assessment

secudit the risk analyzer



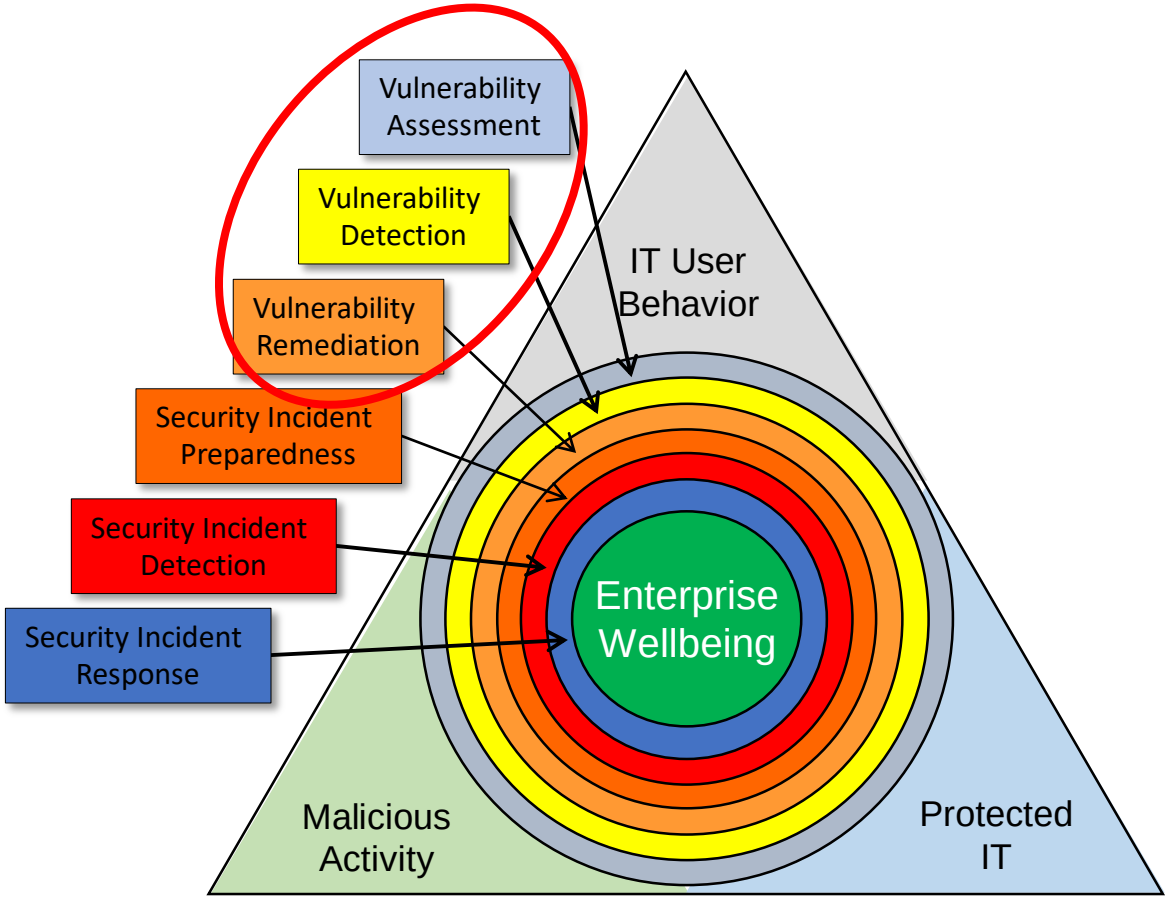
DVA - Distributed Vulnerability Assessment

secudit the risk analyzer



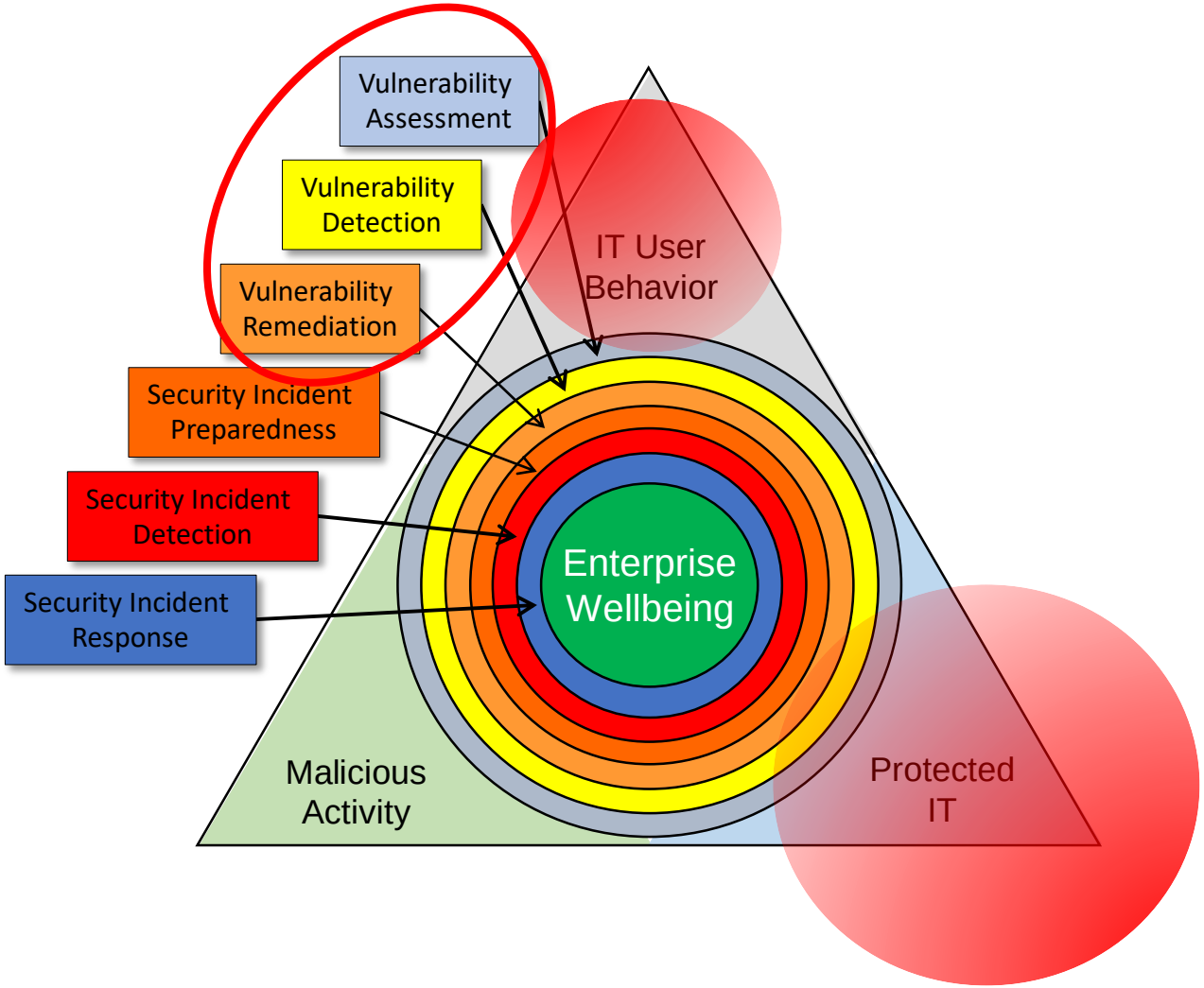
DVA - Distributed Vulnerability Assessment

secudit the risk analyzer



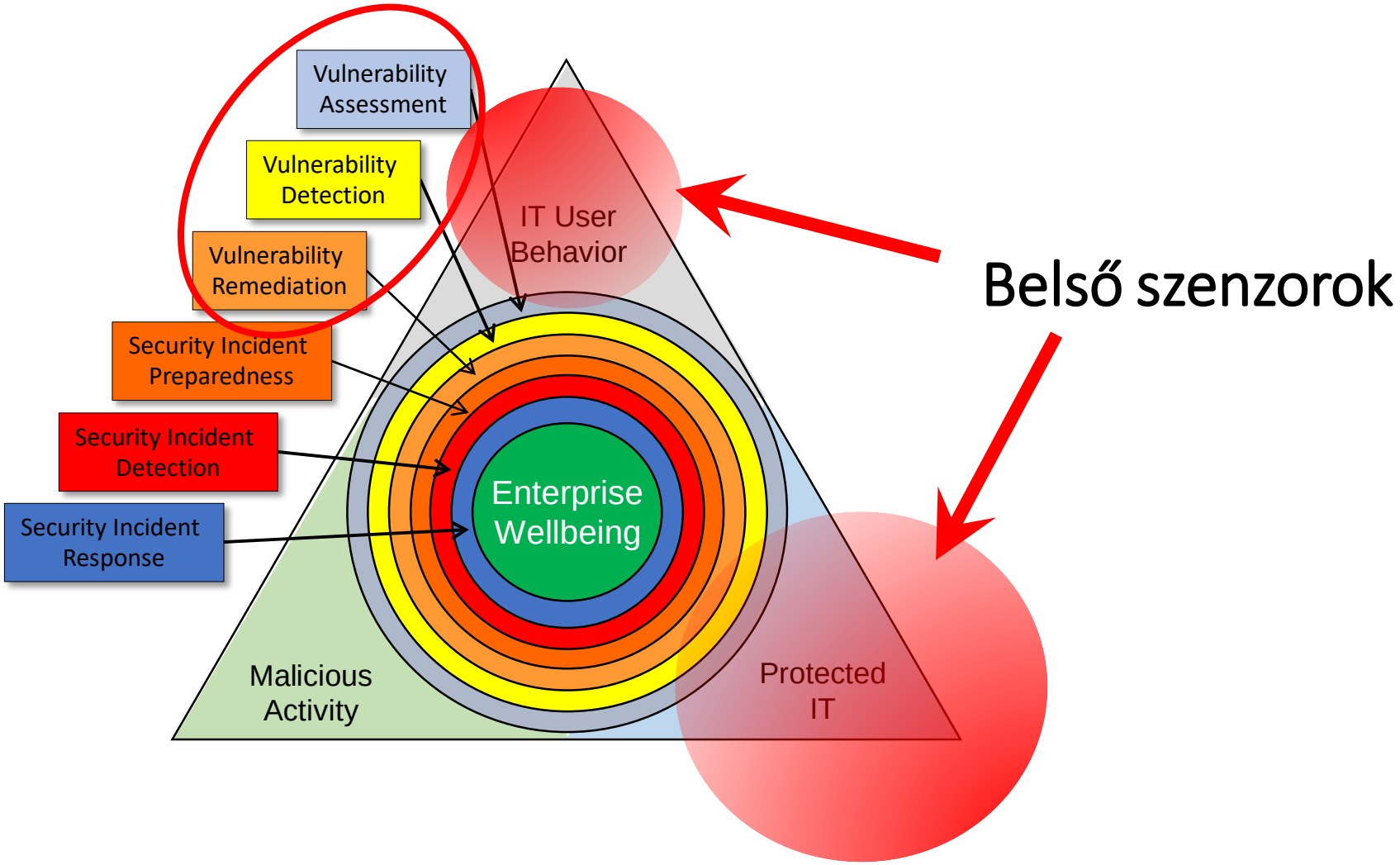
DVA - Distributed Vulnerability Assessment

secudit the risk analyzer



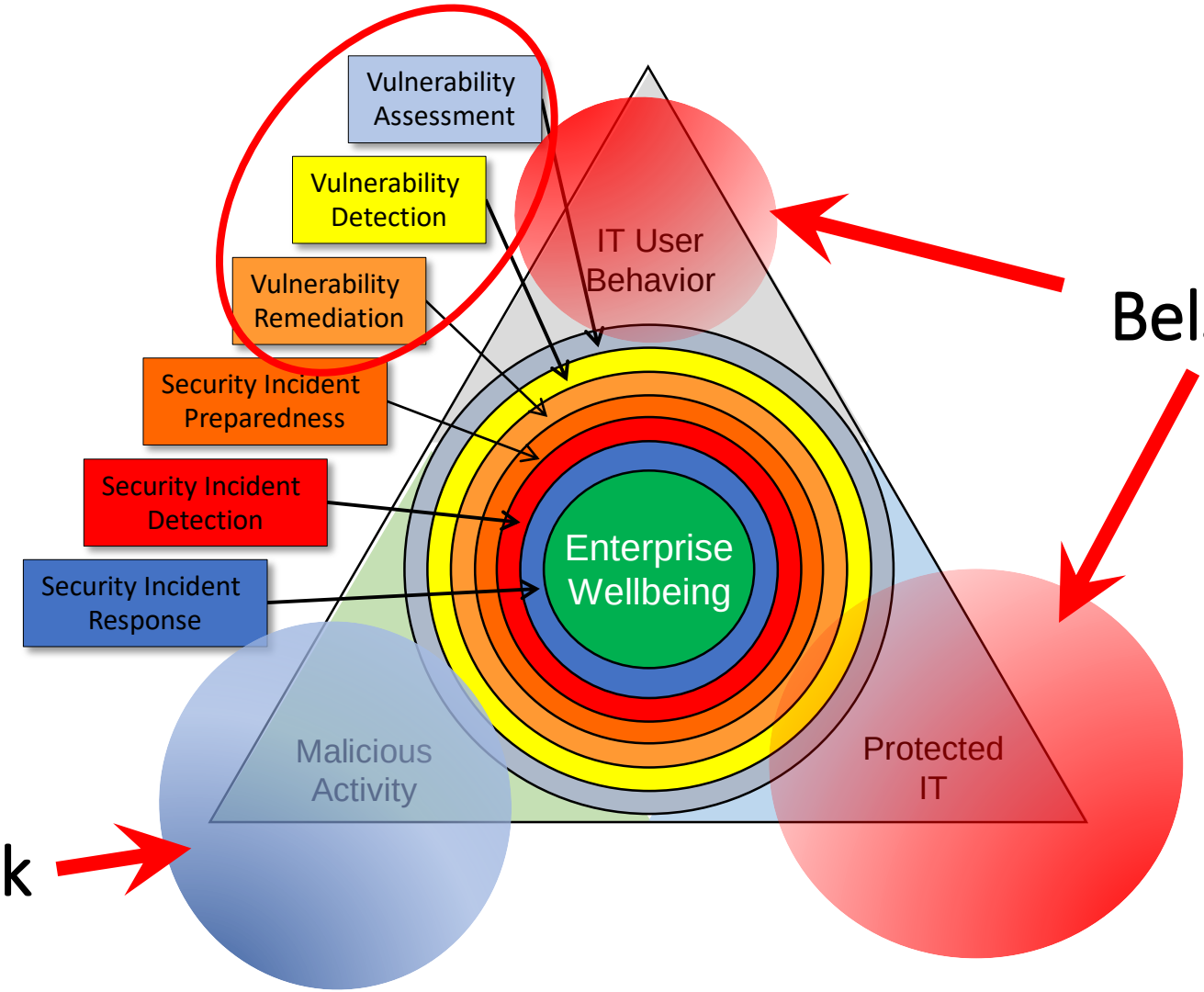
DVA - Distributed Vulnerability Assessment

secudit the risk analyzer



DVA - Distributed Vulnerability Assessment

secudit the risk analyzer

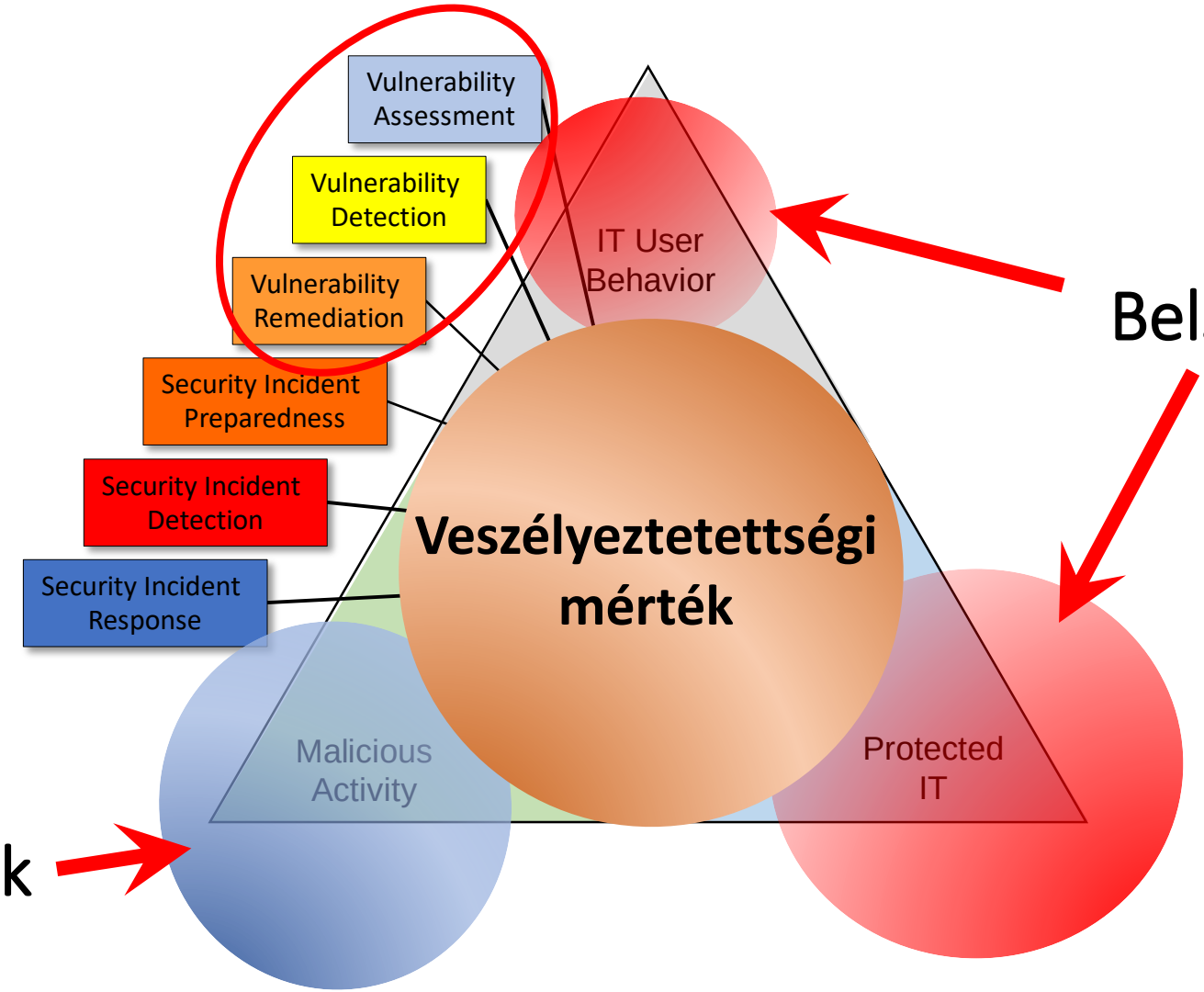


Belső szenzorok

Külső szenzorok

DVA - Distributed Vulnerability Assessment

secudit the risk analyzer



Belső szenzorok

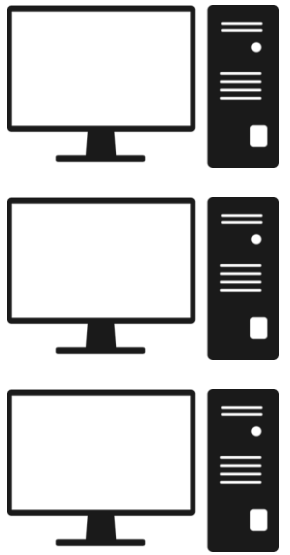
Külső szenzorok

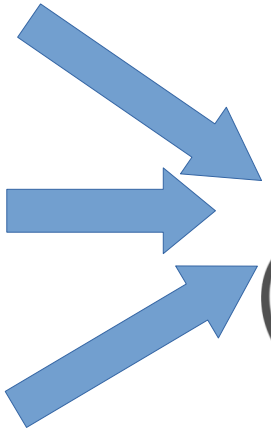
A modell felépítése

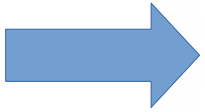
secudit the risk analyzer

Külső szenzorok, előzetes vizsgálatok

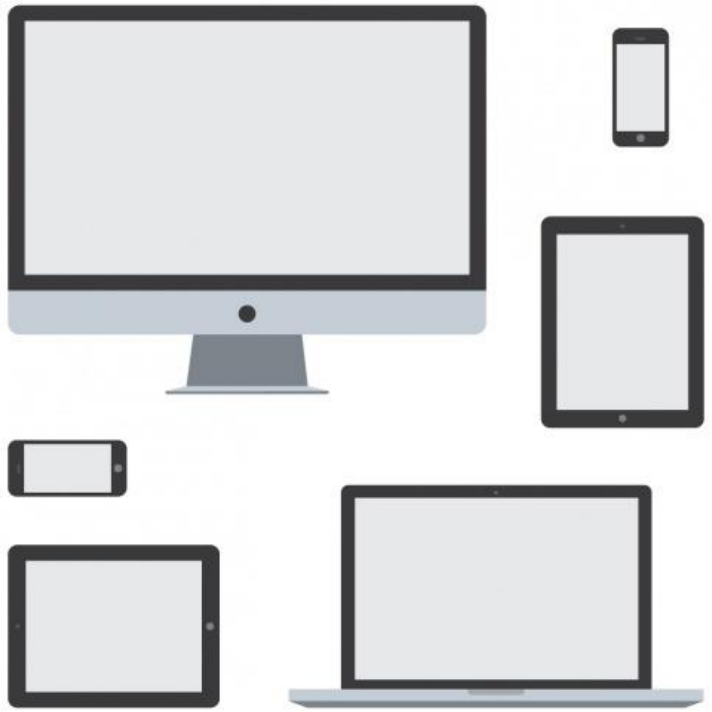
Belső szenzorok







Veszélyeztetettségi metrika



Vizsgálathoz szükséges információk

- IT infrastruktúra információi
- Felhasználói viselkedési információk
- Informatikai fenyegetések információi

Változások követése

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

Felhasználói biztonságtudatosság automatikus figyelése

secudit the risk analyzer

Mit mérjünk?

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

Felhasználói biztonságtudatosság automatikus figyelése

secudit the risk analyzer

Hogyan mérjünk?

Szokásos használat megfigyelése

→ PASSZÍV MÓDSZER

Felhasználói interaktivitás kiváltása, válasz megfigyelése

→ AKTÍV MÓDSZER

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

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

www.secudit.com