DR. LEITOLD FERENC

AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZAT AUTOMATIKUS MENEDZSELÉSE

- ELOSZTOTT FENYEGETETTSÉG FELMÉRÉS

- FELHASZNÁLÓI BIZTONSÁGTUDATOSSÁG AUTOMATIKUS MÉRÉSE

Agenda

Introduction to DVA (Distributed Vulnerability Assessment)

- Concept
- Structure
- Vulnerability metric

Mathematical background of DVA

User-awareness measurement

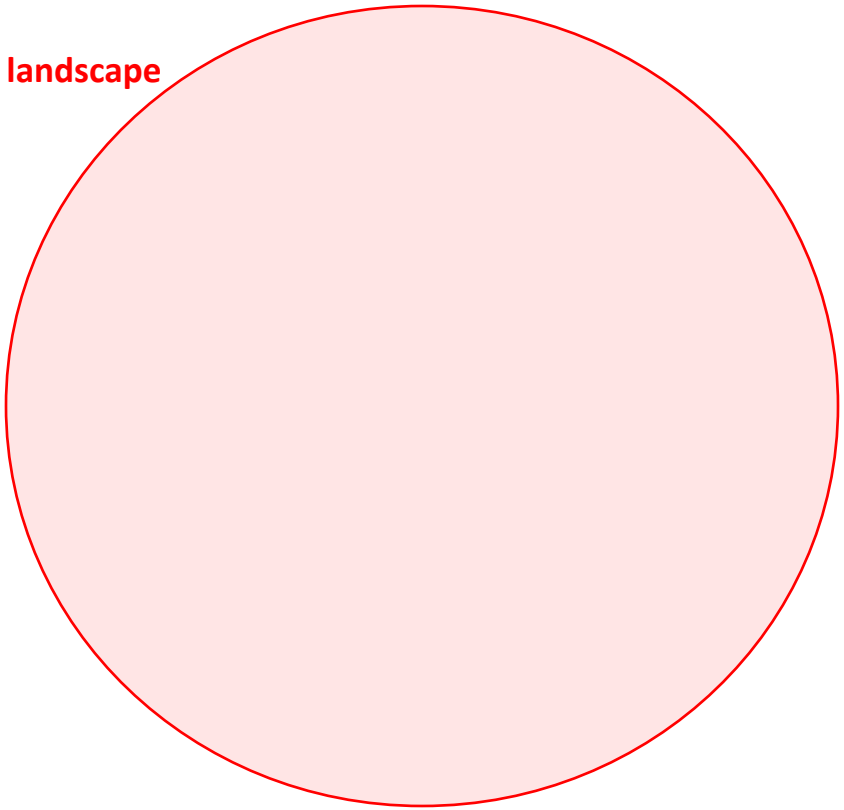
- Concept
- Use(r) cases

AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZAT AUTOMATIKUS MENEDZSELÉSE

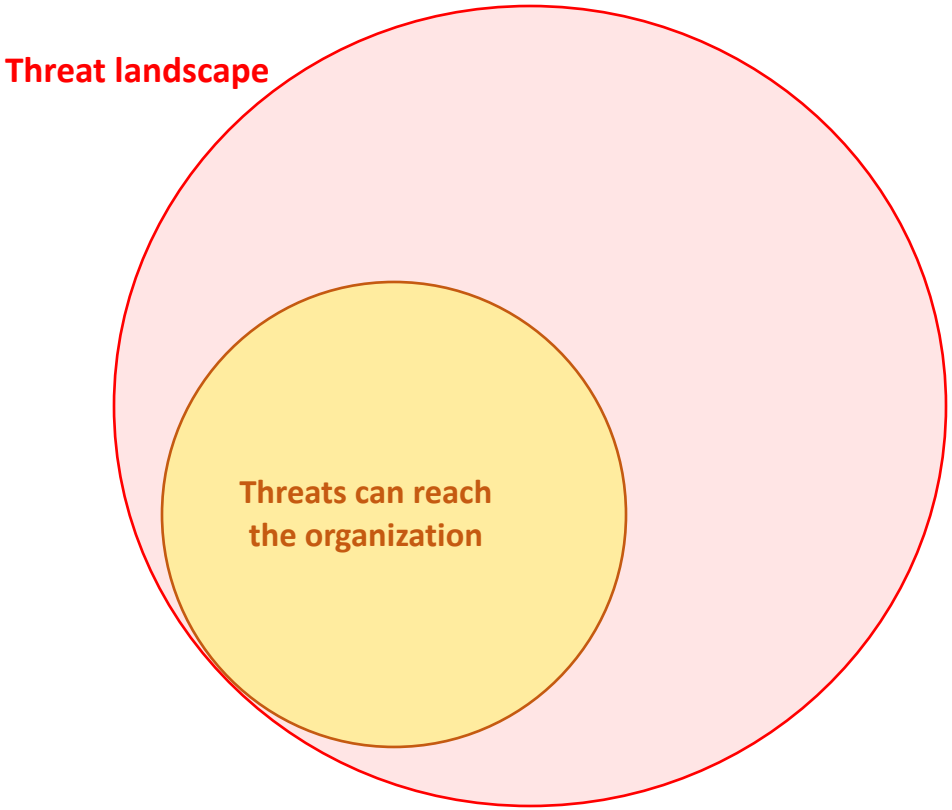

CBCnews | Edmonton
LIVE Edmonton More Streams
Radio One
Listen Live
Home Opinion World Canada Politics Business Health Entertainment Technology & Science Video
Canada Edmonton
Apple watch saved Alberta man's life, makes international headlines
'I bought the watch two weeks before the heart attack, so 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
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 with CBC News
Mobile Facebook Podcasts Twitter Alerts
ADVERTISEMENT
JUNO Award
hosted by michael bu
march 25
find out mo
Weather
Wednesday Thursday Friday Saturday
1°C -2°C -2°C -3°C
Sunday

Distributed Vulnerability Assessment

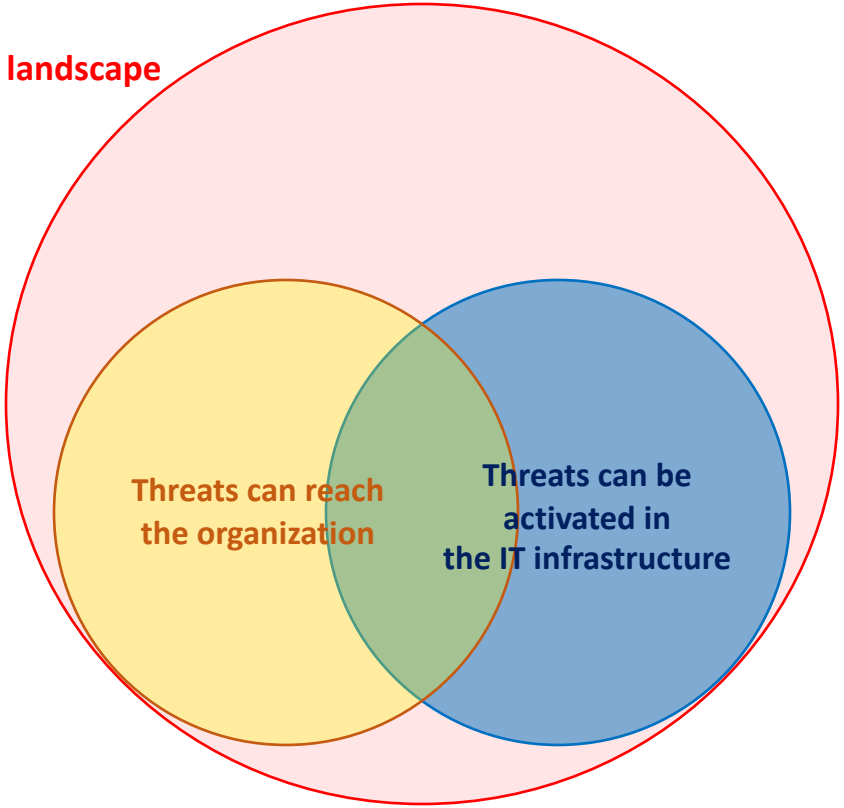
Distributed Vulnerability Assessment



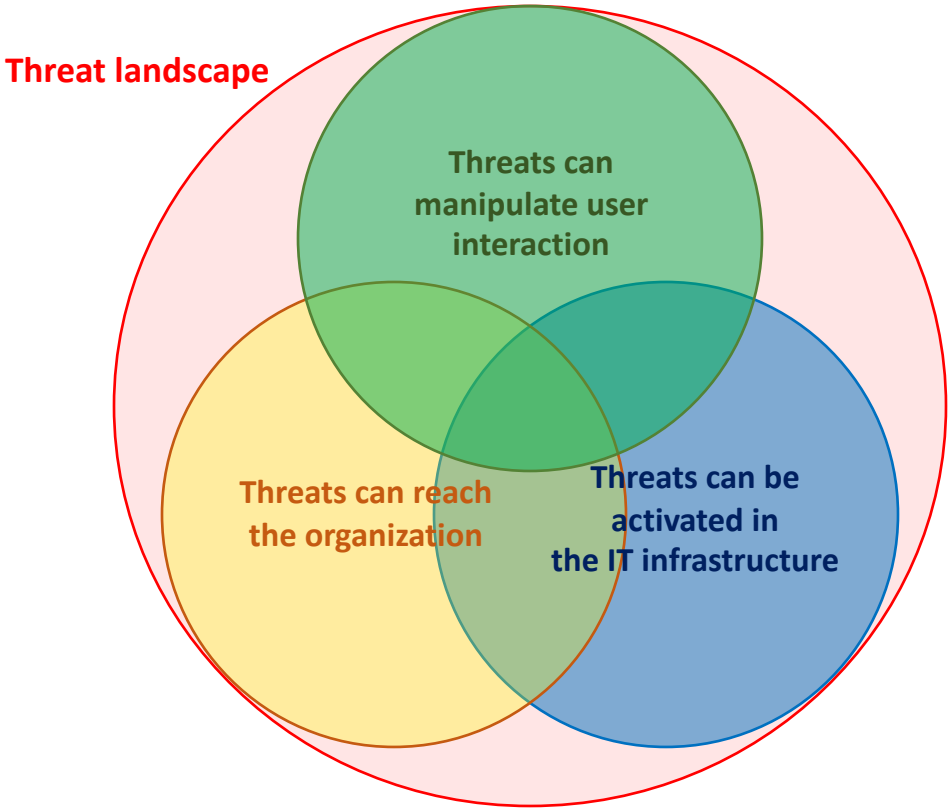
Distributed Vulnerability Assessment



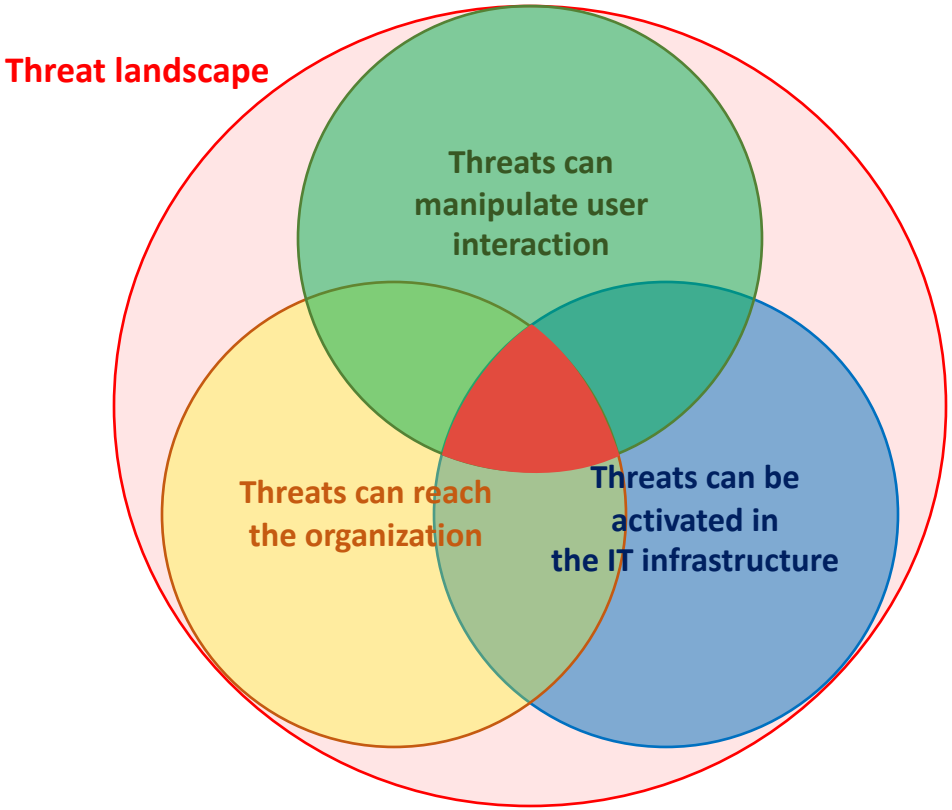
Distributed Vulnerability Assessment



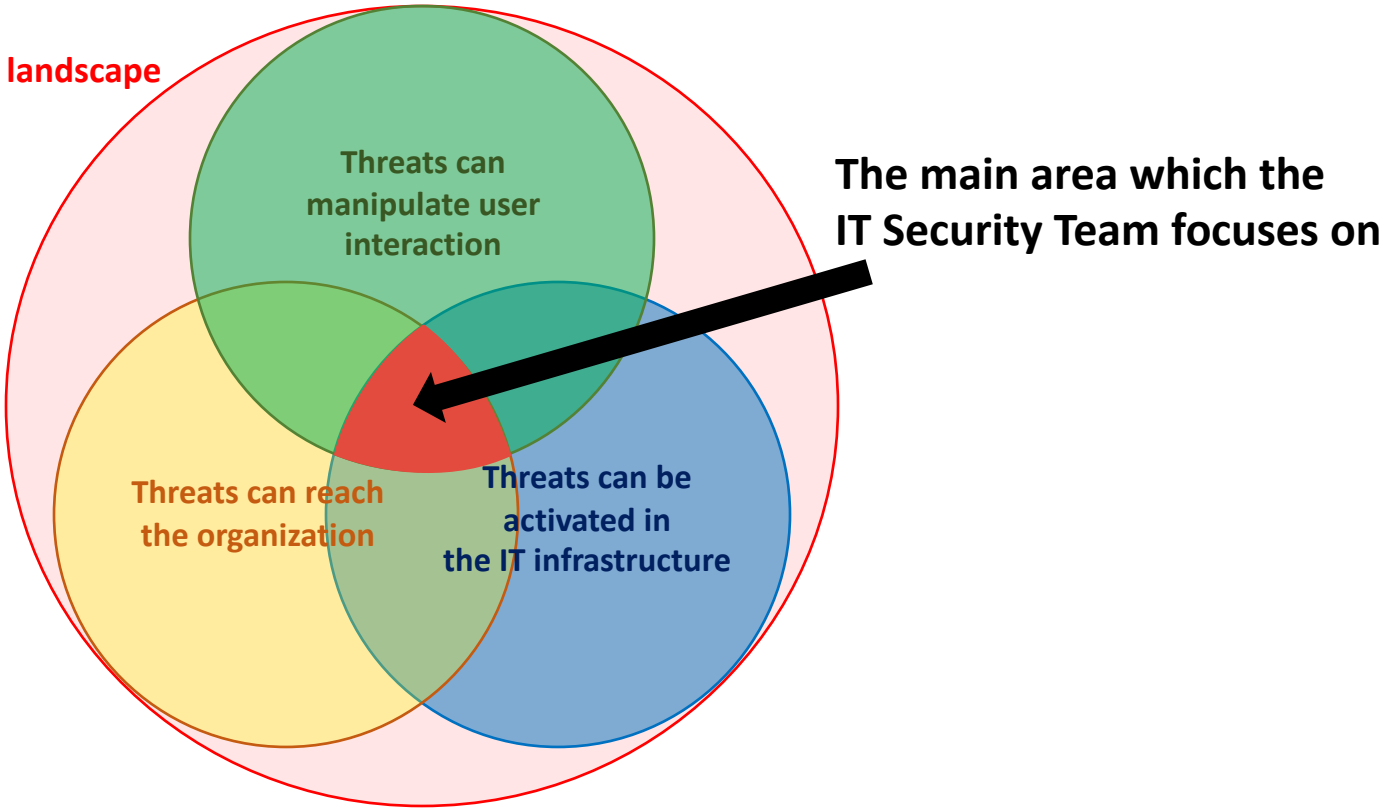
Distributed Vulnerability Assessment



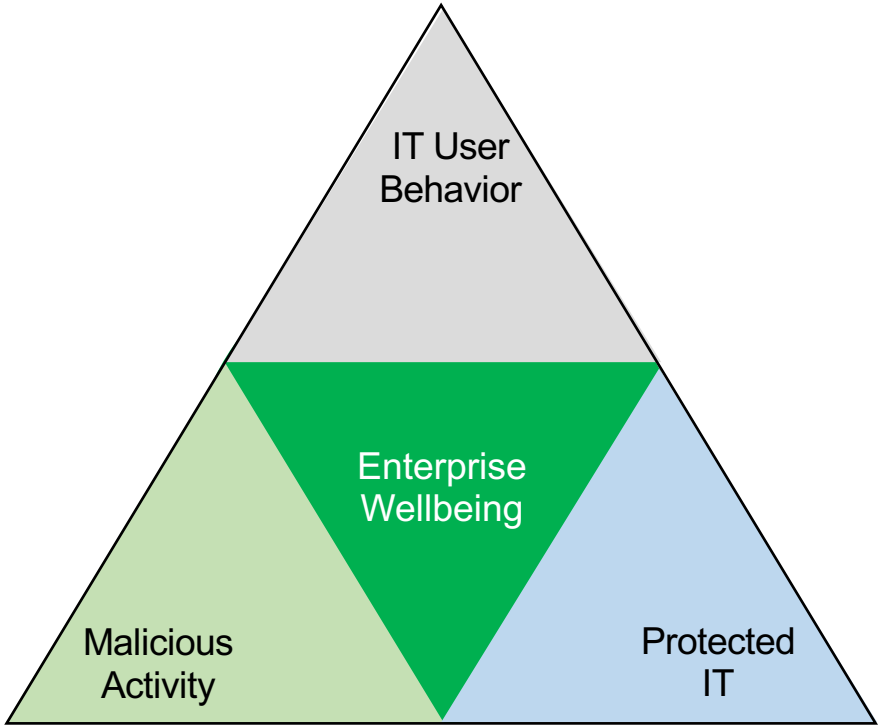
Distributed Vulnerability Assessment



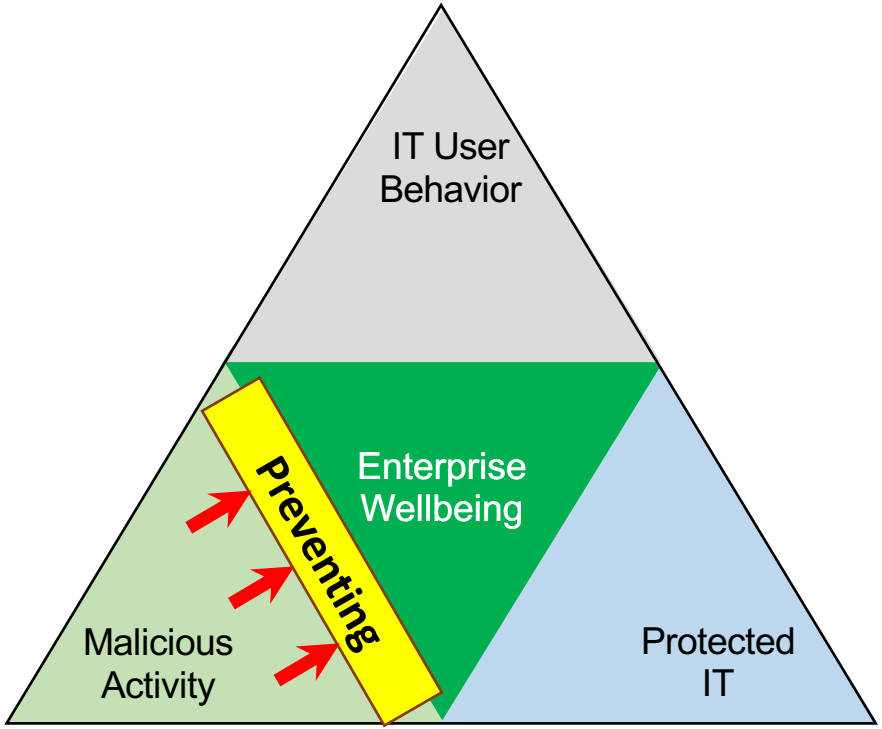
Distributed Vulnerability Assessment



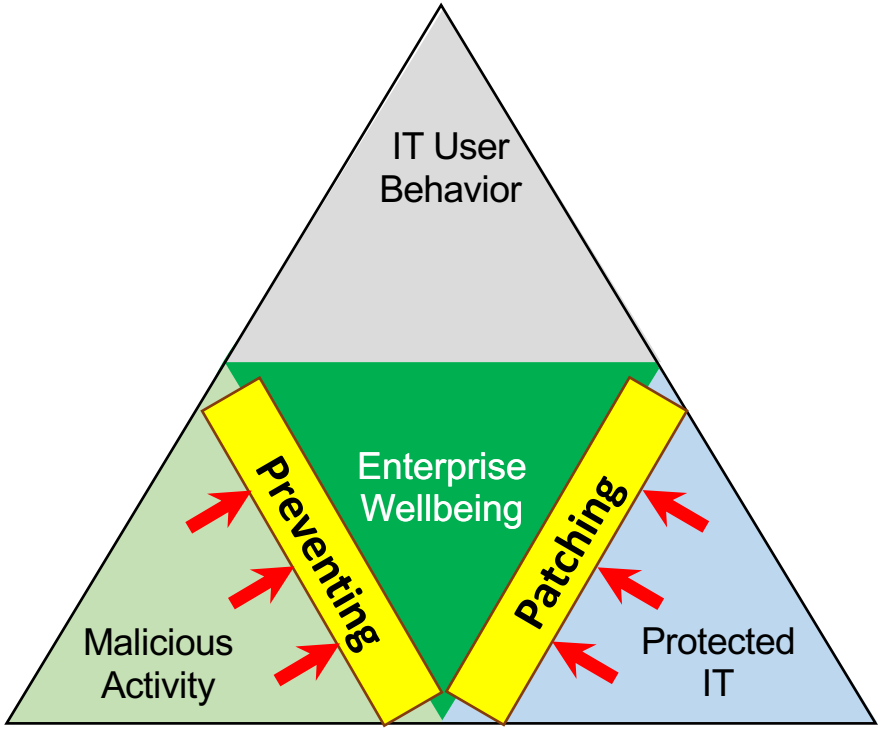
Distributed Vulnerability Assessment



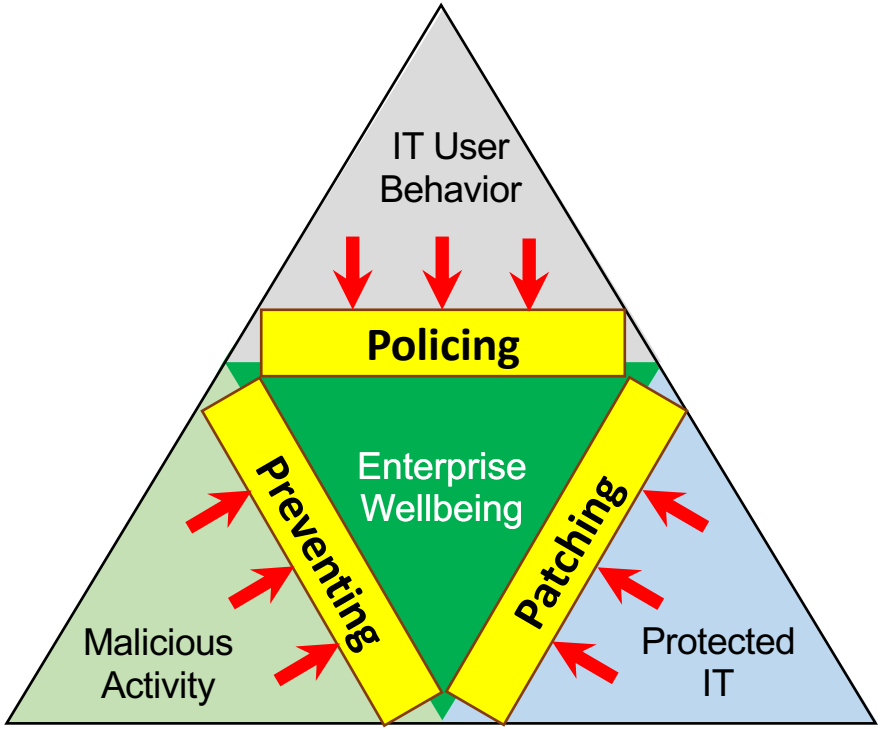
Distributed Vulnerability Assessment



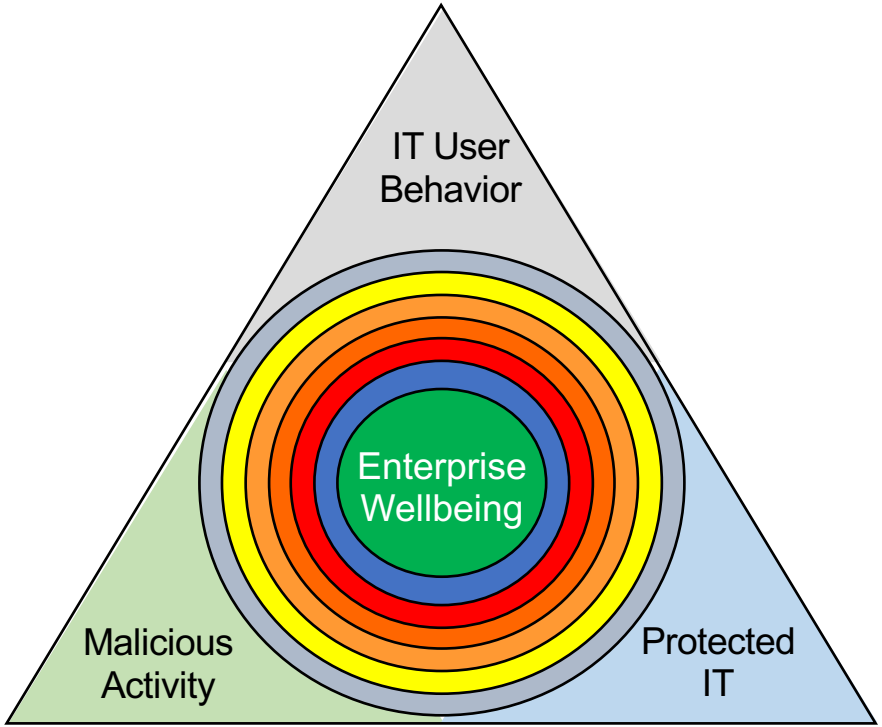
Distributed Vulnerability Assessment



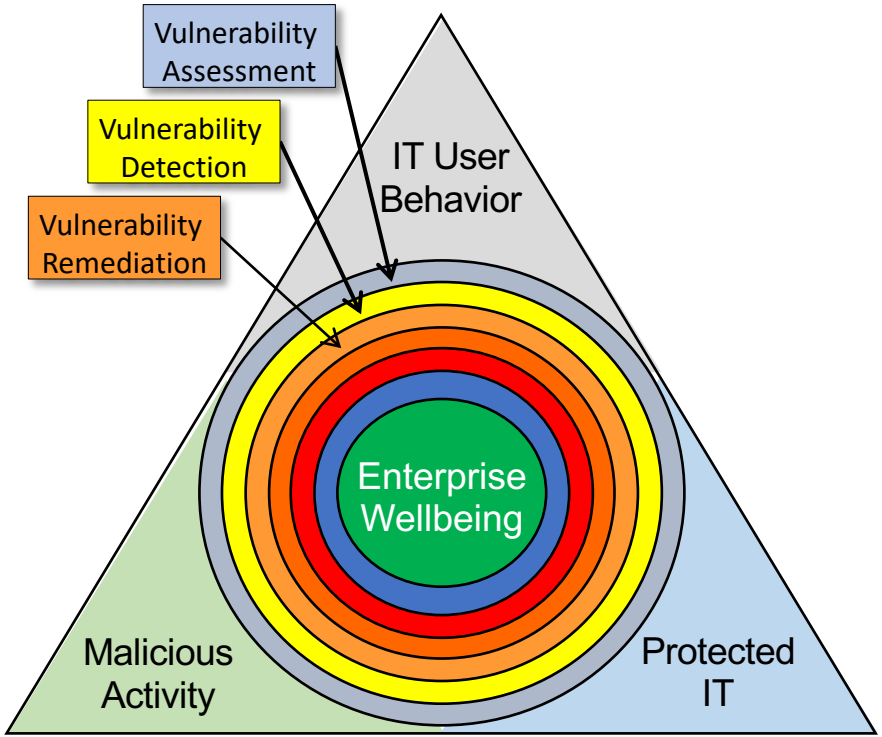
Distributed Vulnerability Assessment



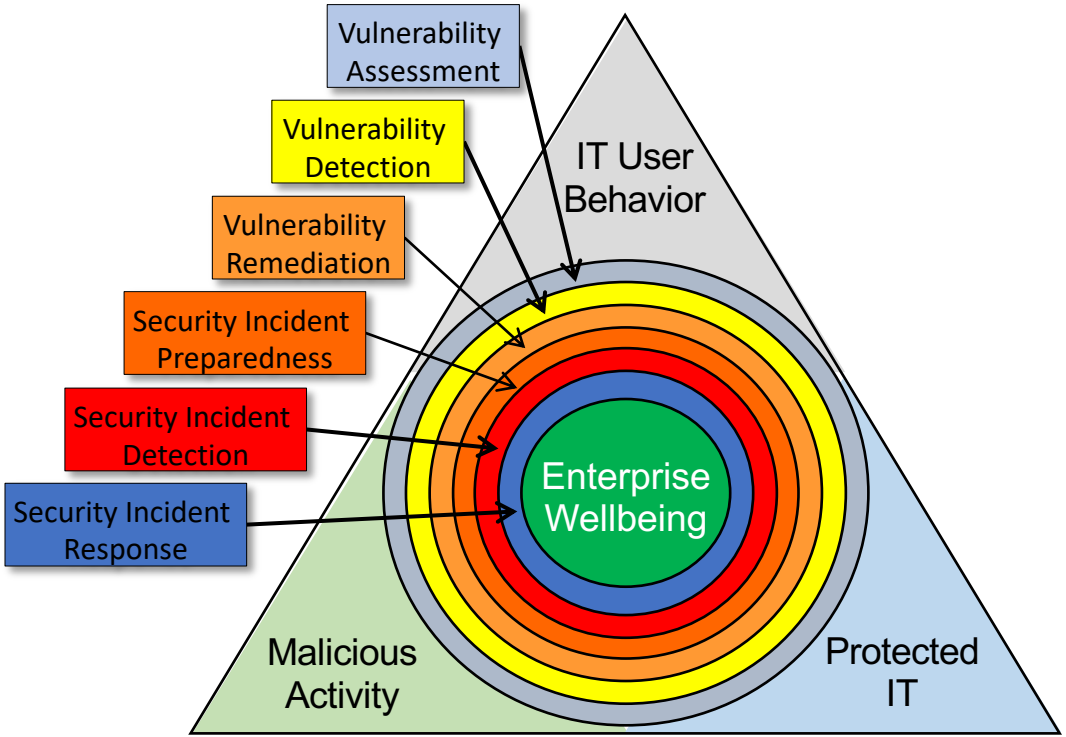
Distributed Vulnerability Assessment



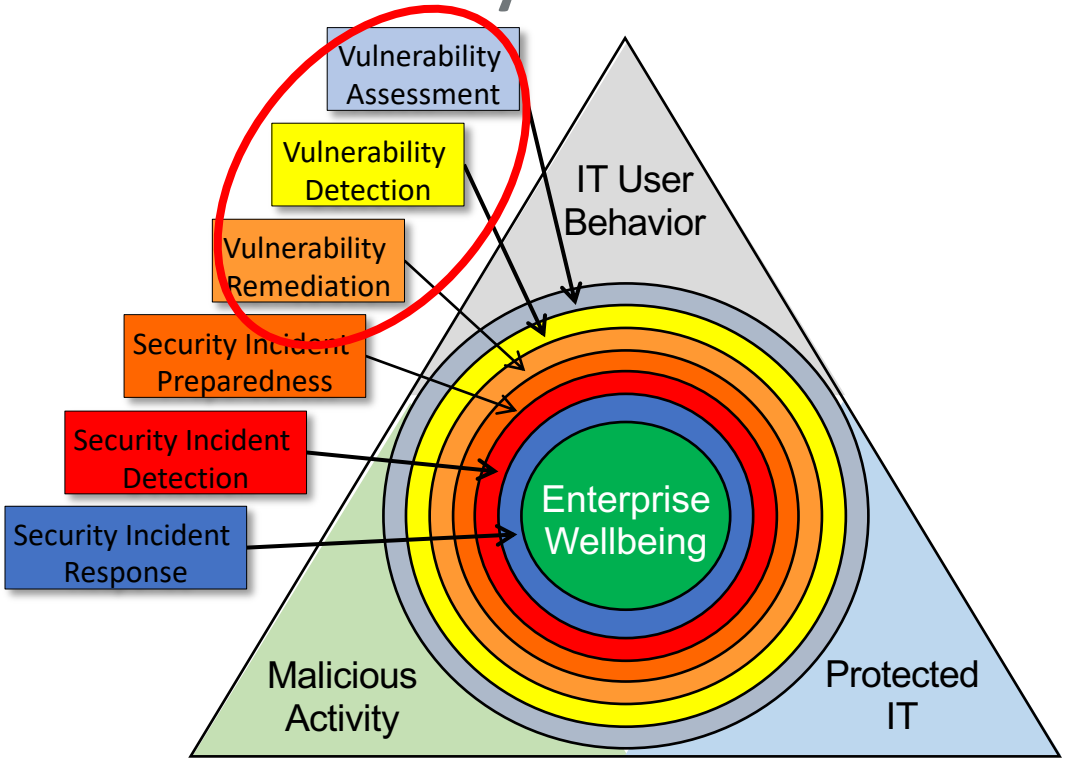
Distributed Vulnerability Assessment



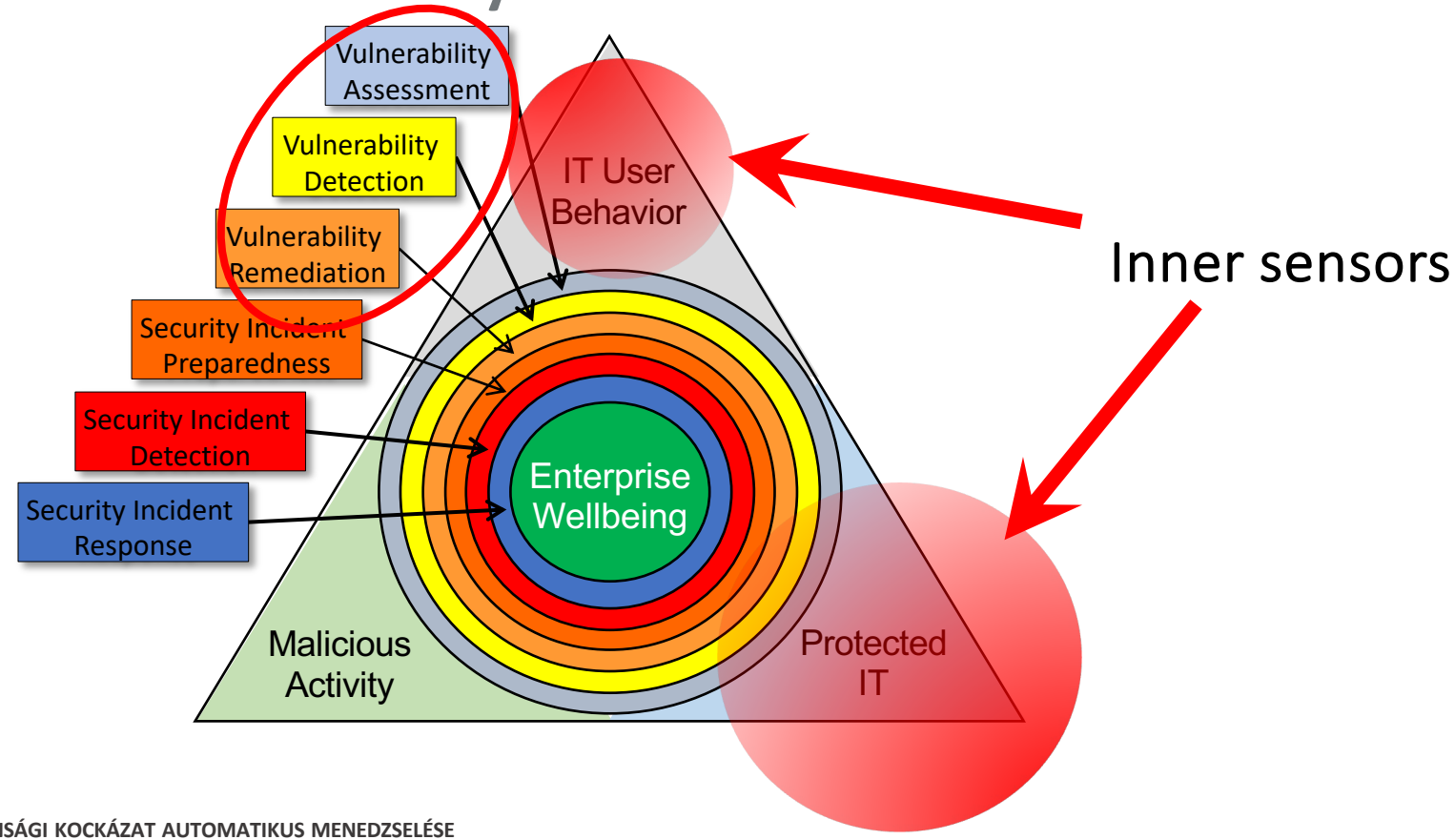
Distributed Vulnerability Assessment



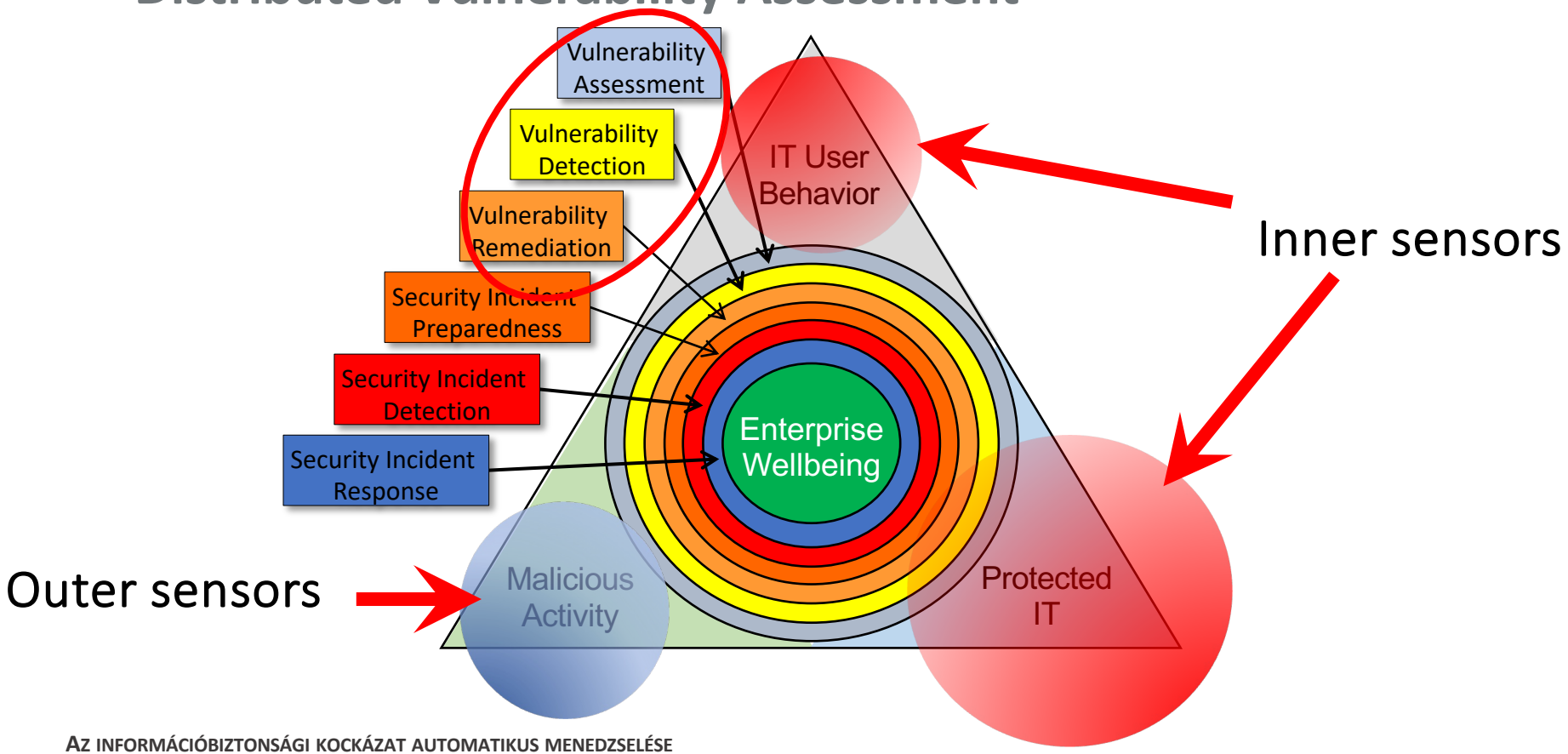
Distributed Vulnerability Assessment



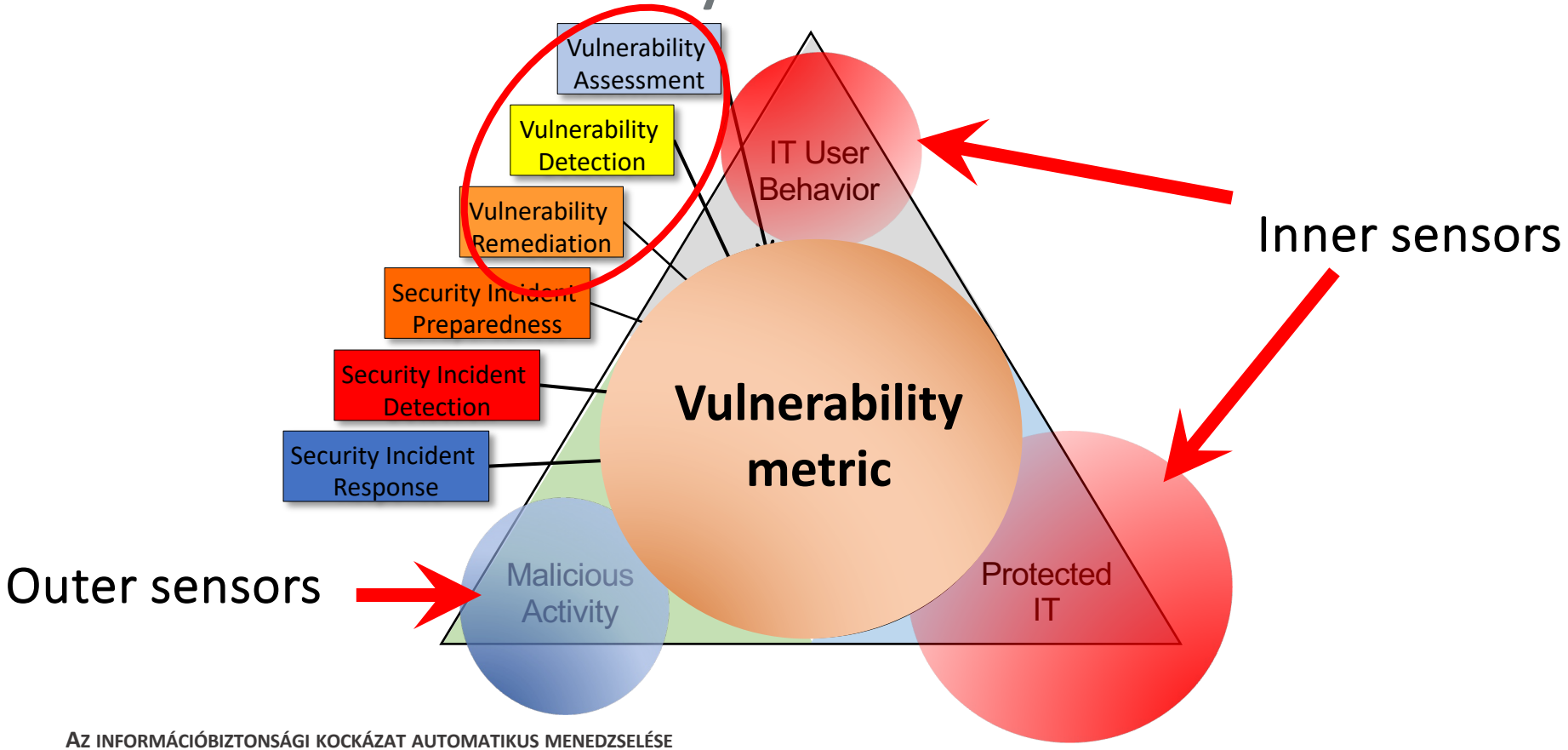
Distributed Vulnerability Assessment



Distributed Vulnerability Assessment



Distributed Vulnerability Assessment



Vulnerability metric

- customized metrics
- identify vulnerable IT elements
- identify dangerous users’ behavior
- estimate different contributions (user/device/threat groups)
- “what if” estimations, recommendations

Mathematical background

K. Hadarics, F. Leitold:
Improving distributed vulnerability assessment model of cybersecurity
Central and Eastern European e|Dem¸and e|Gov Days 2018
Conference proceedings, Wien, Ausztria : Facultas Verlags- und Buchhandels AG, (2018) pp. 385-394. , 10 p.

K. Hadarics, F. Leitold. A. Arrott:
Distributed vulnerability assessment applied to measuring citizen cyberhealth and securing online public services
Central and Eastern European e|Dem and e|Gov Days 2017, Budapest, Hungary

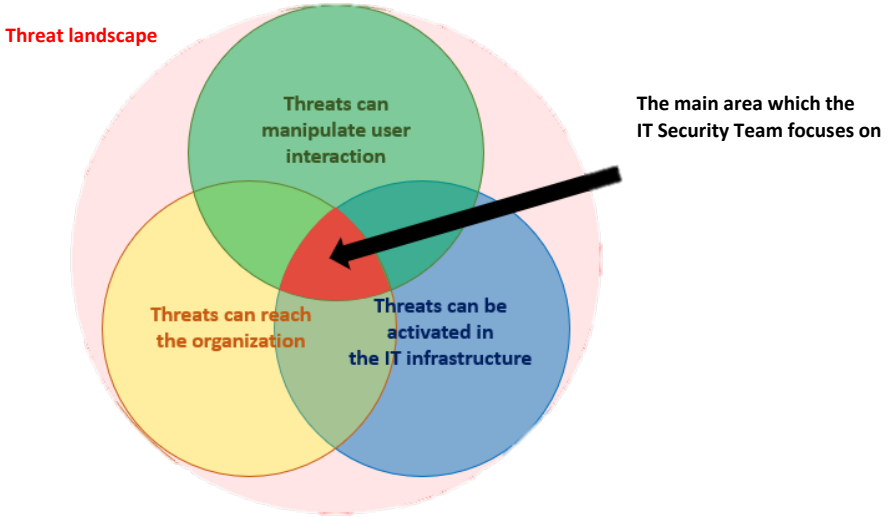
K. Hadarics, K. Győrffy, B. Nagy, L. Bognár, A. Arrott, F. Leitold:
Mathematical Model of Distributed Vulnerability Assessment
9th International Scientific Conference, Security and Protection of Information, 2017, Brno, Czech Republic

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

Mathematical background

Triunal Model of

Cybersecurity Vulnerability

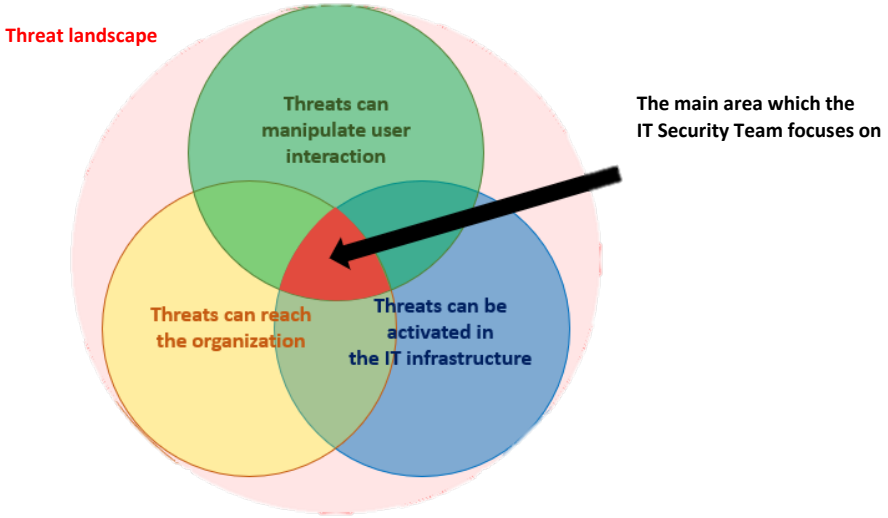


Three contributing sources, or triunes:

- malicious activity
- unprotected IT
- facilitating adverse user behavior

Mathematical background

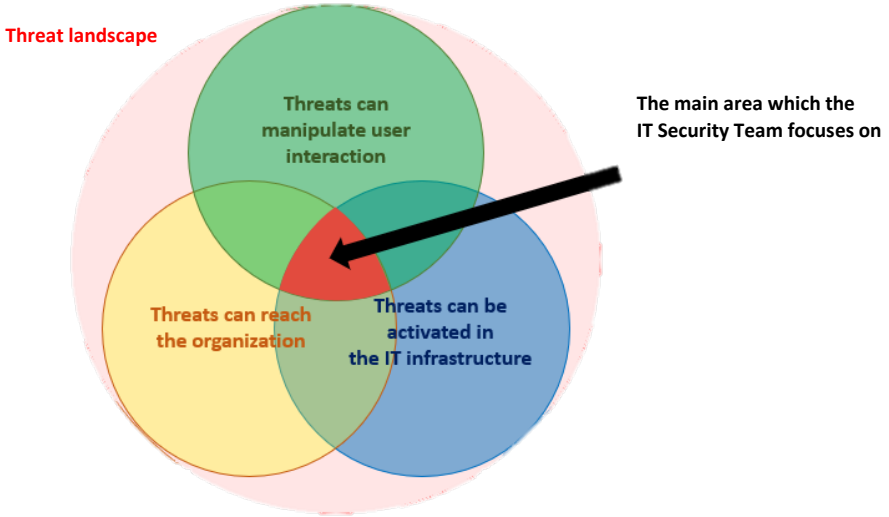
Estimating vulnerability level



Mathematical background

Estimating vulnerability level

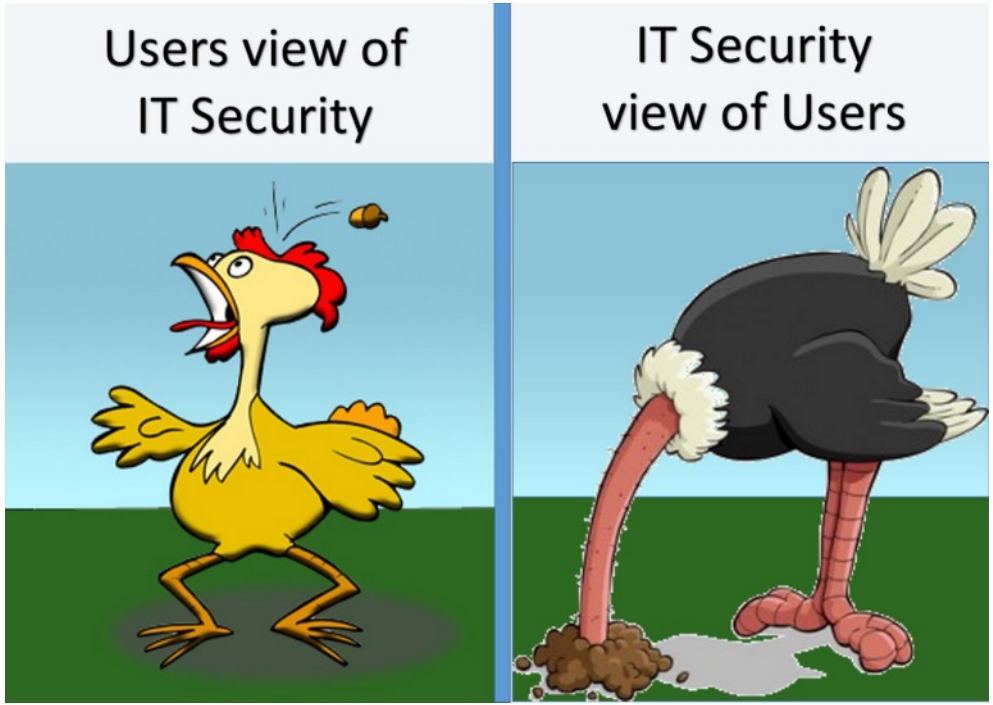
The vulnerability level of the infrastructure is defined as **the probability of at least one threat** capable of **reaching the organization** and being executed on **at least one device** used by **the given users** in the infrastructure.



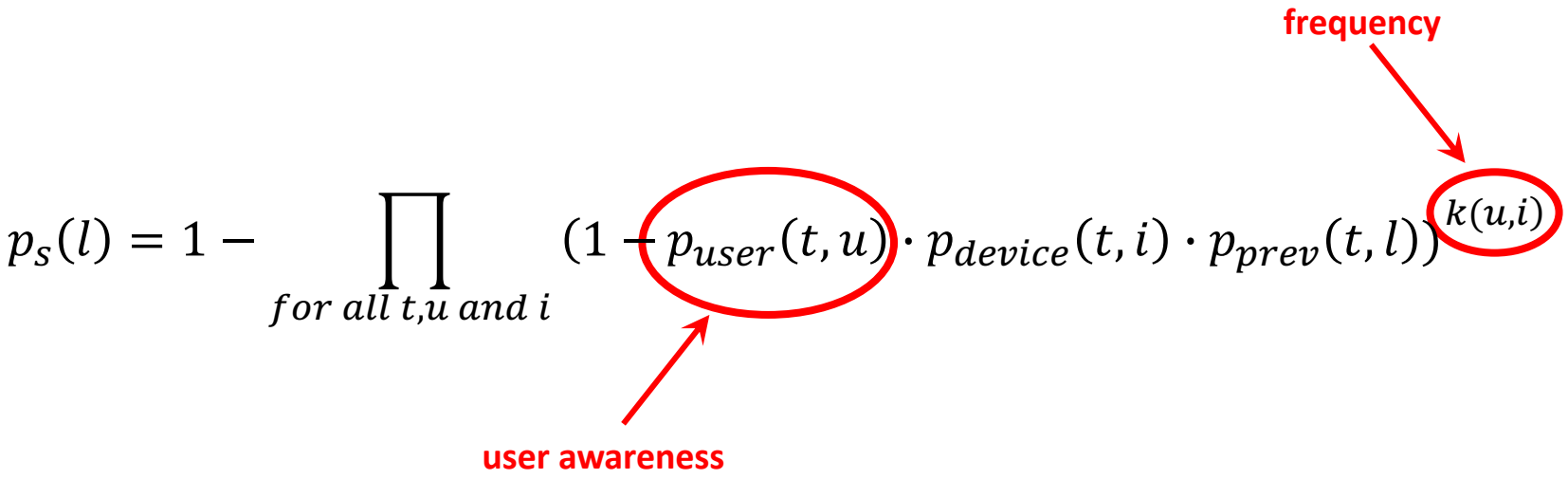
Mathematical background

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

User awareness measurement – why is it important?



User awareness measurement



User awareness measurement

What can we measure?

- Device usage
- Application usage (especially: for communication)
- Opening different types of files
- Influence protections (e.g.: update policy, suspension)
- Browsing on the internet
- …

User awareness measurement

How can we measure?

PASSIVE

monitoring normal usage

ACTIVE

causing different situations

User awareness measurement – use(r) cases

Case I: Different browsing habits

In the browser he opens only www.cnn.com and www.wheather.com websites.

In the browser she opens at least 20 new websites a week which have not been visited in the previous 6 months by her.

User awareness measurement – use(r) cases

Case II: Different occupation

Working at the HR department, she receives job applications by email, including CVs in PDF attachments.

He has never received any email with PDF attachment before.

User awareness measurement – use(r) cases

Case III: Mixture of case I & II

Threat I.

Working at the HR department, she receives job applications by email, including CVs in PDF attachments.

In the browser she opens only www.cnn.com and www.wheather.com websites.

He has never received any email with PDF attachment before.

In the browser he opens at least 20 new websites a week which have not been visited in the previous 6 months by him.

Threat II.

User awareness measurement – use(r) cases

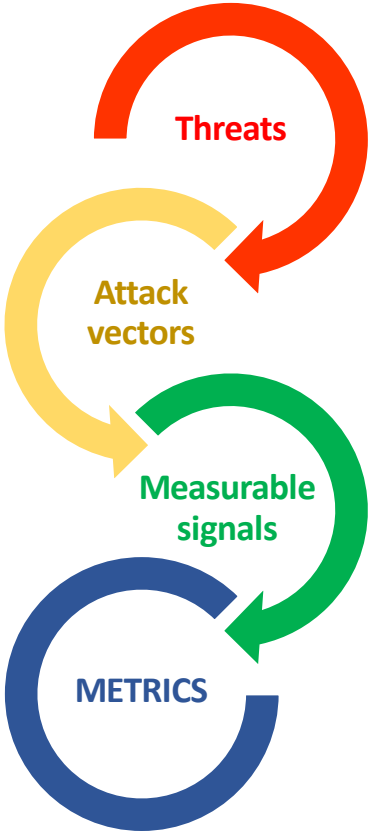
Conclusions

- User awareness measurement has to be distributed related to different attack vectors
- Distributed measurement can be used for calculating the integrated metric related to the security level of the organization …
- … and it can be used for organizing customized actions for the users

User awareness measurement – research

Research project has been started

- to identify user interaction characteristics in the case of different **threats** and to group them by **attack vectors**,
- to identify **measurable signals** having any connection with user actions,
- to find correlation between user actions identified by relevant **signals** and **attack vectors**,
- to define **metrics** related to user behavior level for each **attack vector**.



AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZAT AUTOMATIKUS MENEDZSELÉSE