Védelmi rendszerek vizsgálatának problémái

Dr. Leitold Ferenc

Veszprog Kft., CheckVir tesztlabor

28 évvel ezelőtt

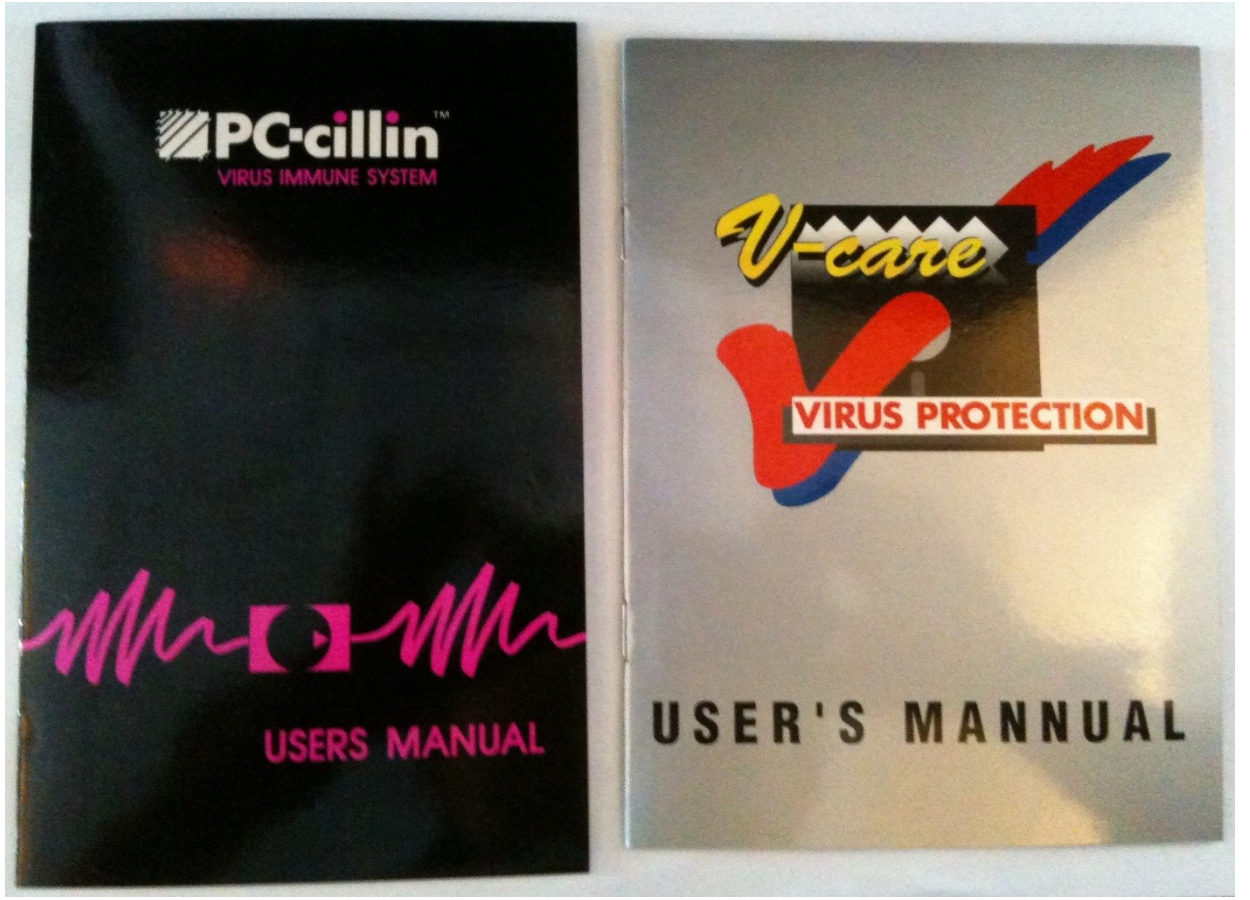
Potyogós / Cascade vírus (1988)

- 1701 – 1704 byte
- COM és EXE fájlokat fertőz
- oligomorf
- “potyogó betűk”

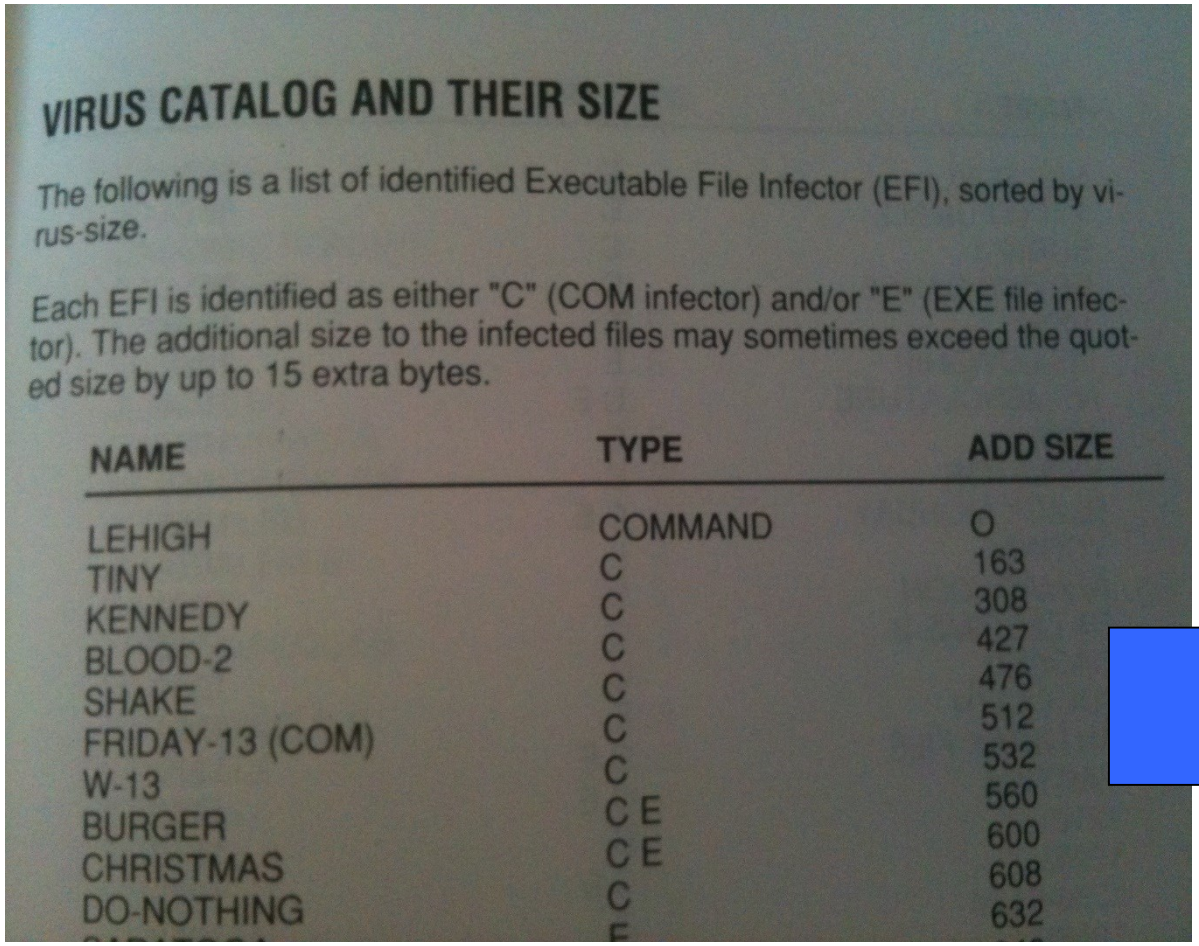
SCAN.EXE (1989)

- 18 (!) különböző vírus felismerése
- Csak felismerés, helyreállítás nélkül
- Csak ha elindítjuk, nincs folyamatos védelem
- DOS operációs rendszer alatt

1-2 évvel később



A V-Care leírásban



VIRUS CATALOG AND THEIR SIZE

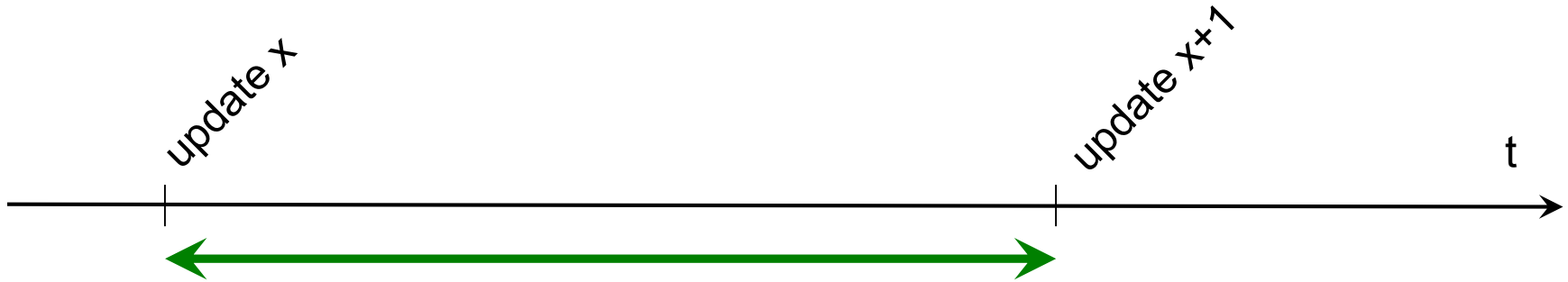
The following is a list of identified Executable File Infector (EFI), sorted by virus-size.

Each EFI is identified as either "C" (COM infector) and/or "E" (EXE file infector). The additional size to the infected files may sometimes exceed the quoted size by up to 15 extra bytes.

NAME	TYPE	ADD SIZE
LEHIGH	COMMAND	O
TINY	C	163
KENNEDY	C	308
BLOOD-2	C	427
SHAKE	C	476
FRIDAY-13 (COM)	C	512
W-13	C	532
BURGER	C E	560
CHRISTMAS	C E	600
DO-NOTHING	C	608
		632

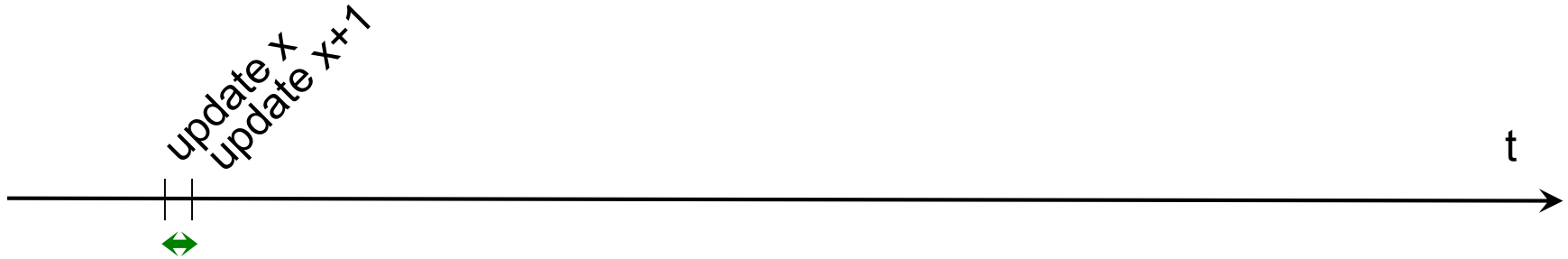
105 vírus listája

Védelmek frissítései (90-es évek eleje)



Két egymást követő frissítés között eltelt idő elég arra, hogy a védelem minden védelmi eljárását és minden funkcióját megvizsgáljuk minden létező kártevővel szemben.

Védelmek frissítései (2011)



A teljes vizsgálat lehetetlen.
A konzekvens működés, a reprodukálhatóság sem működik.

Védelmi rendszerek (2016)

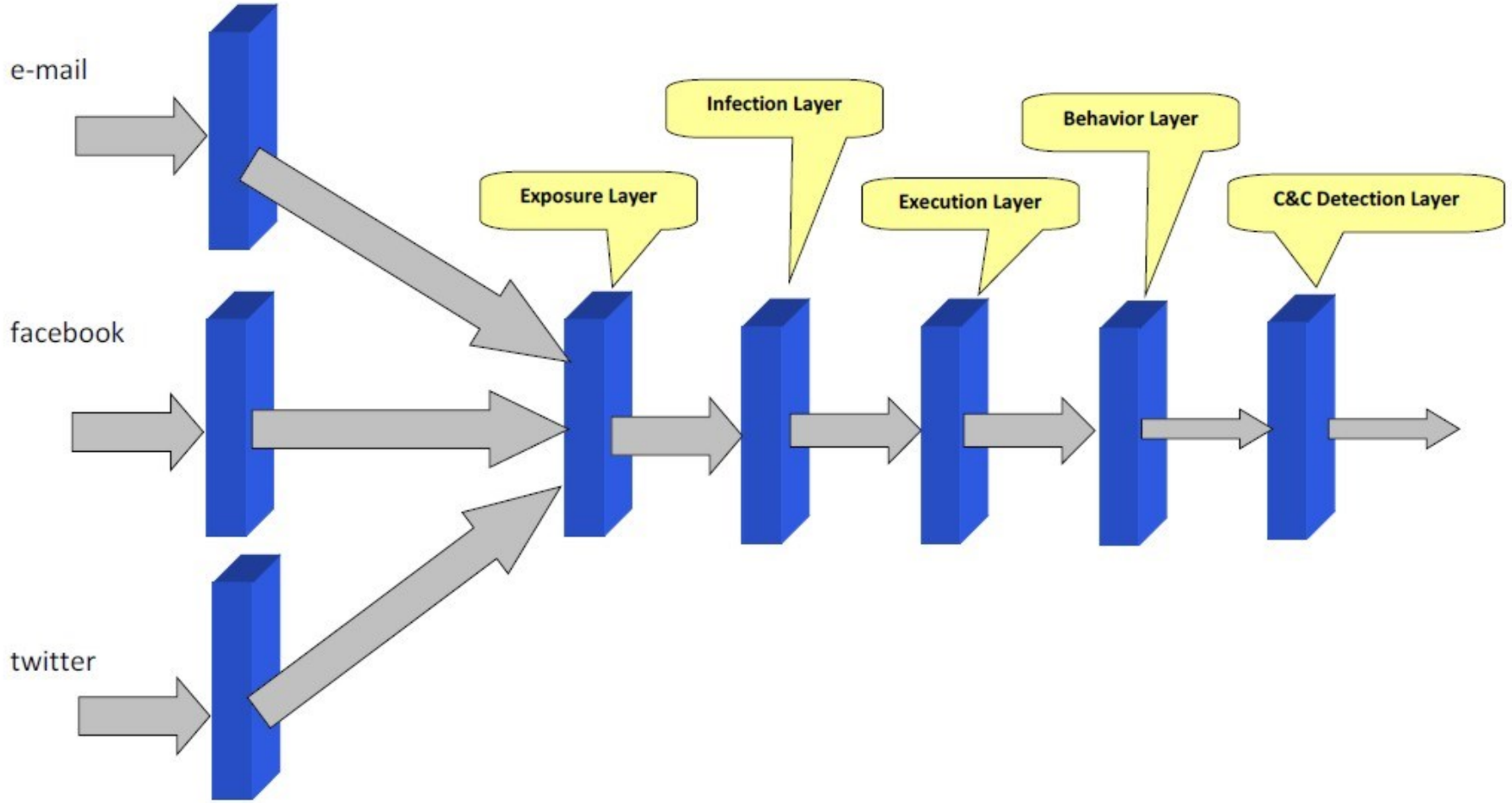
- Több százmillió kártevő kezelése
- Több védelmi eljárás, rengeteg funkció
- Komplex működés
- Folyamatosan változik (felhő technológia)

☞ **nehéz vizsgálat, szakértelmet igényel**

☞ **nem reprodukálható**

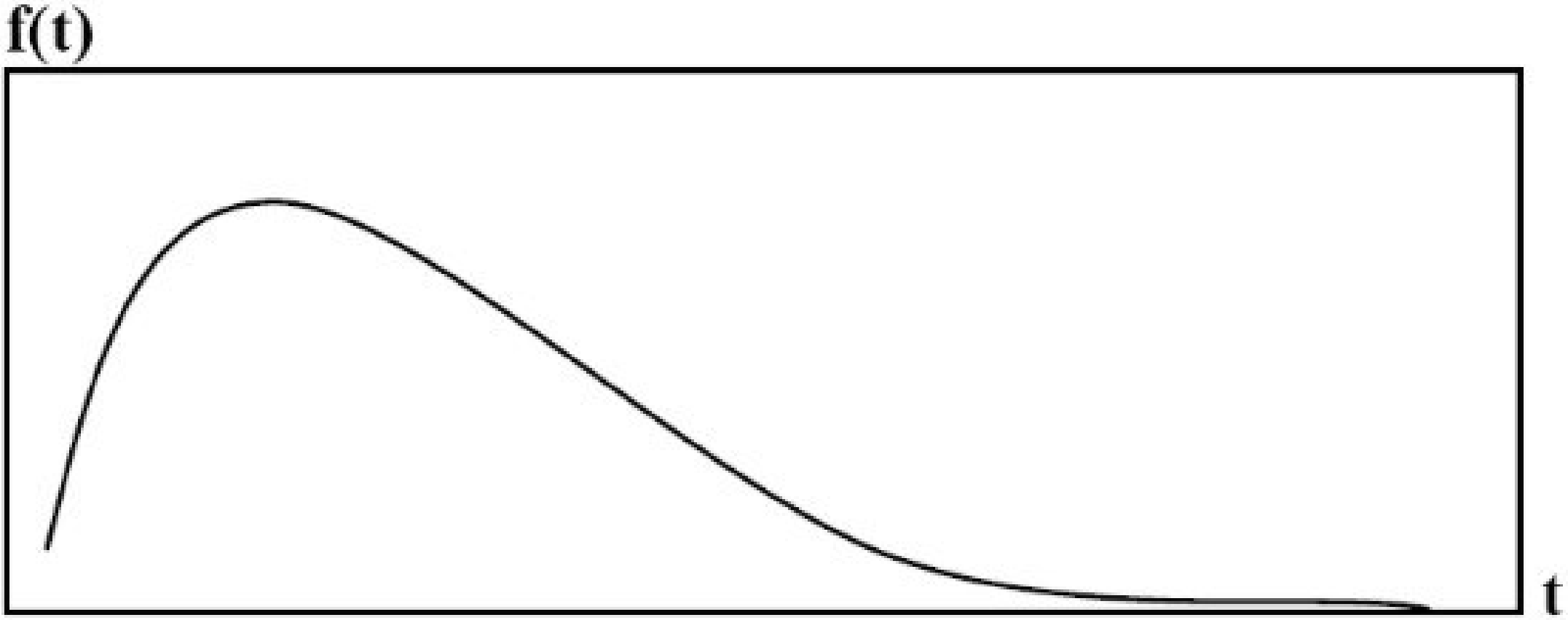
☞ **gyártói befolyásolás lehetősége**

Többszintű védelmek



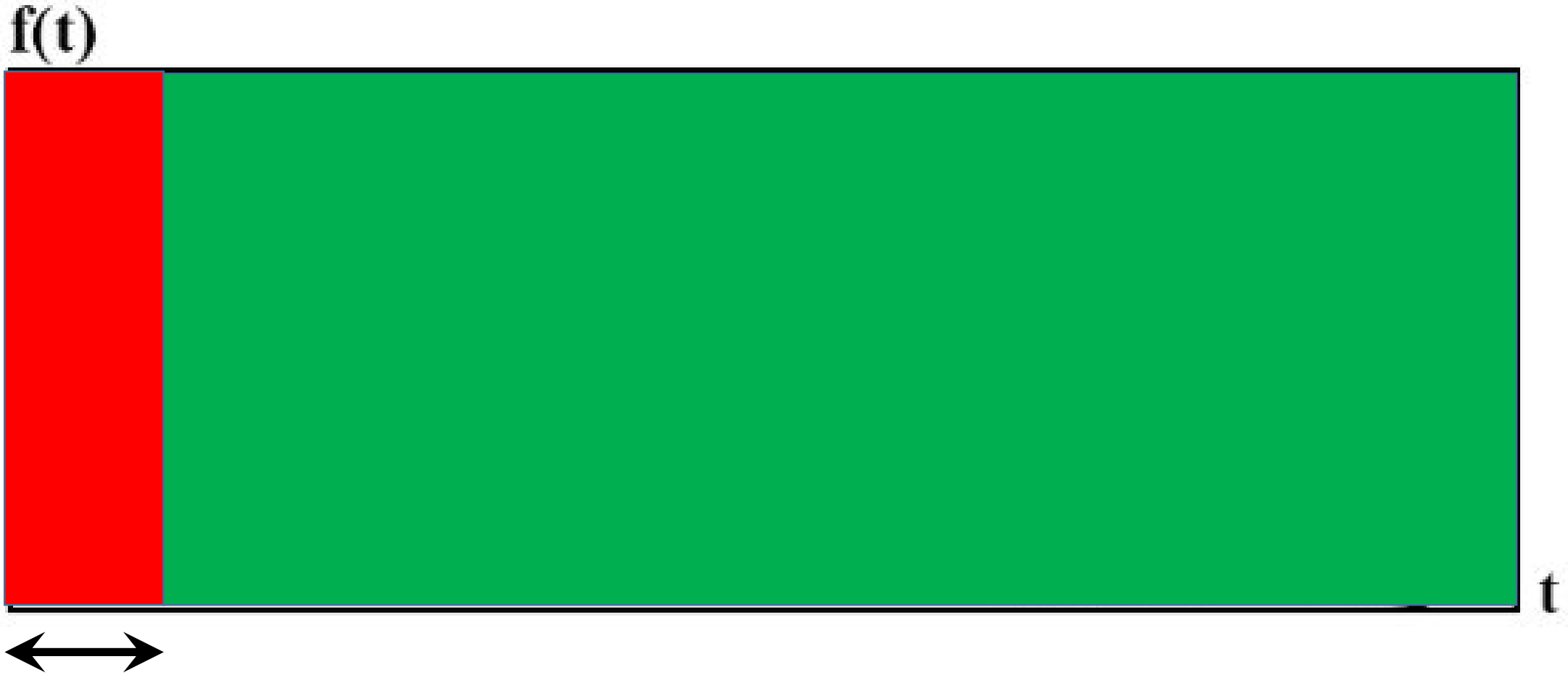
Kártevők élettartama

Kártevők élettartama

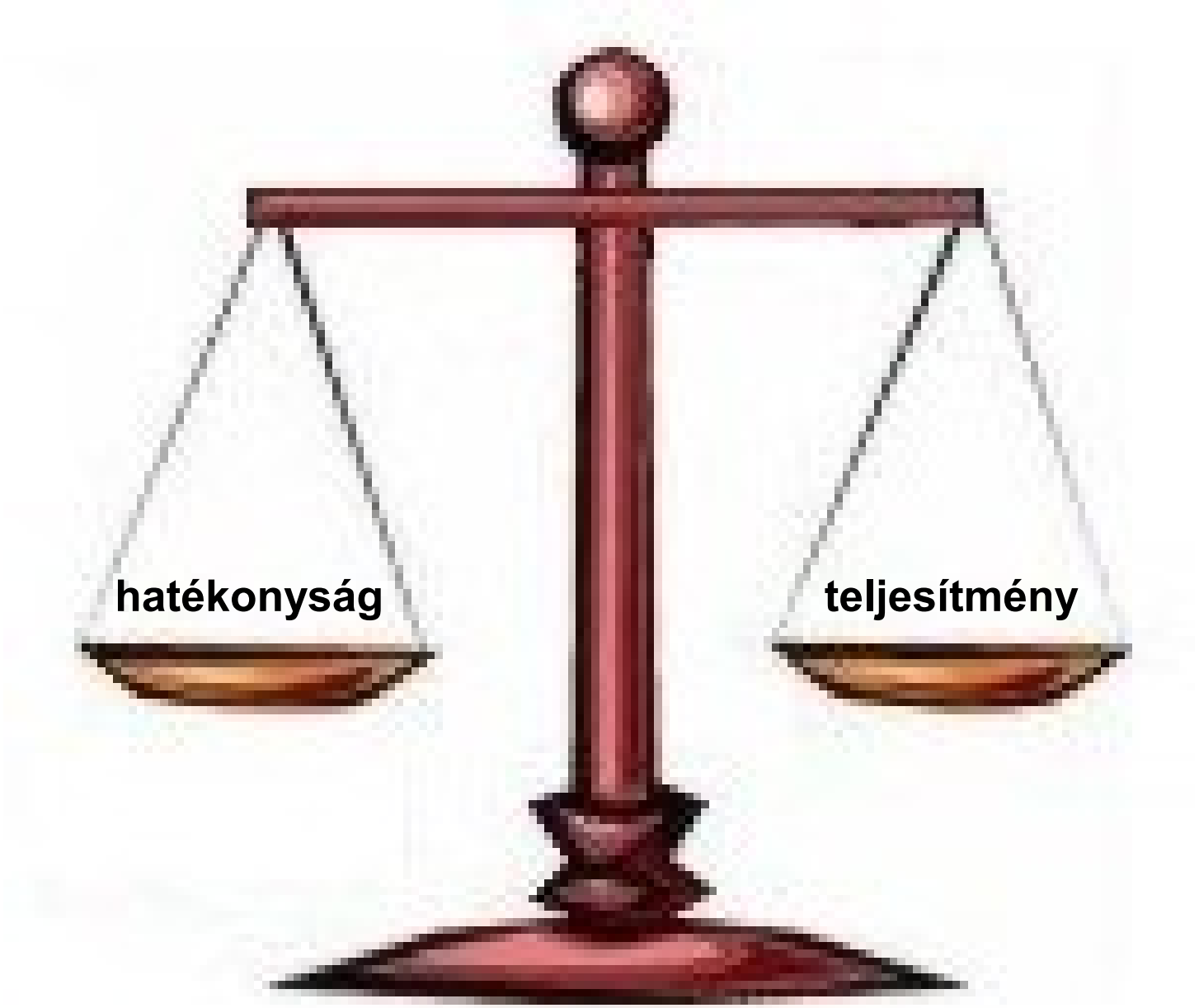


Kártevők élettartama

Kártevők élettartama



Vizsgálati szempontok



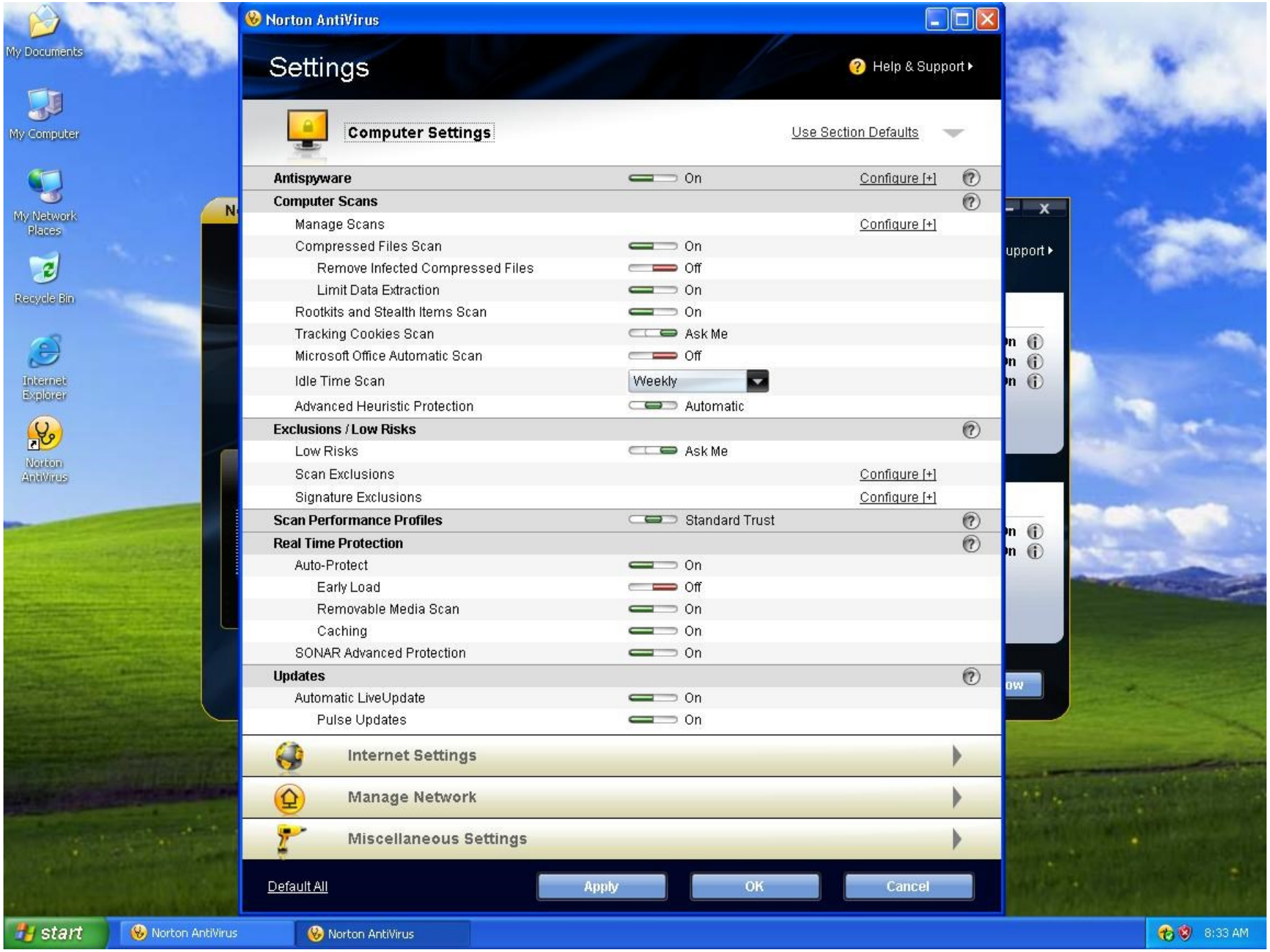
Vizsgálati eljárások

Bootolási idő tesztelése

Mi a fontosabb?

BOOTOLÁSI IDŐ vagy BIZTONSÁGOS BOOTOLÁS

DEMO

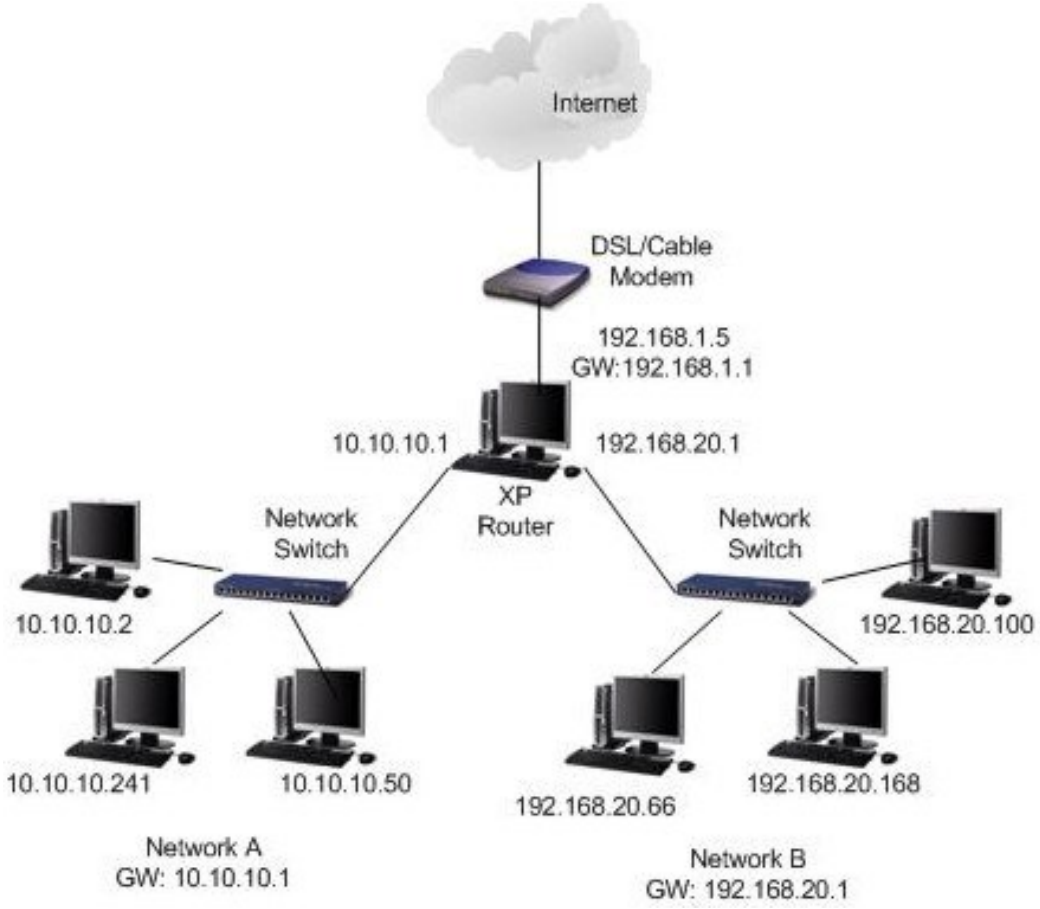

My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Norton AntiVirus
Norton AntiVirus
Settings
Help & Support
Computer Settings
Use Section Defaults
Antispyware On Configure [+]
Computer Scans
Manage Scans Configure [+]
Compressed Files Scan On
Remove Infected Compressed Files Off
Limit Data Extraction On
Rootkits and Stealth Items Scan On
Tracking Cookies Scan Ask Me
Microsoft Office Automatic Scan Off
Idle Time Scan Weekly
Advanced Heuristic Protection Automatic
Exclusions / Low Risks
Low Risks Ask Me
Scan Exclusions Configure [+]
Signature Exclusions Configure [+]
Scan Performance Profiles Standard Trust
Real Time Protection
Auto-Protect On
Early Load Off
Removable Media Scan On
Caching On
SONAR Advanced Protection On
Updates
Automatic LiveUpdate On
Pulse Updates On
Internet Settings
Manage Network
Miscellaneous Settings
Default All
Apply
OK
Cancel
start
Norton AntiVirus
Norton AntiVirus
8:33 AM

CHECKVIR

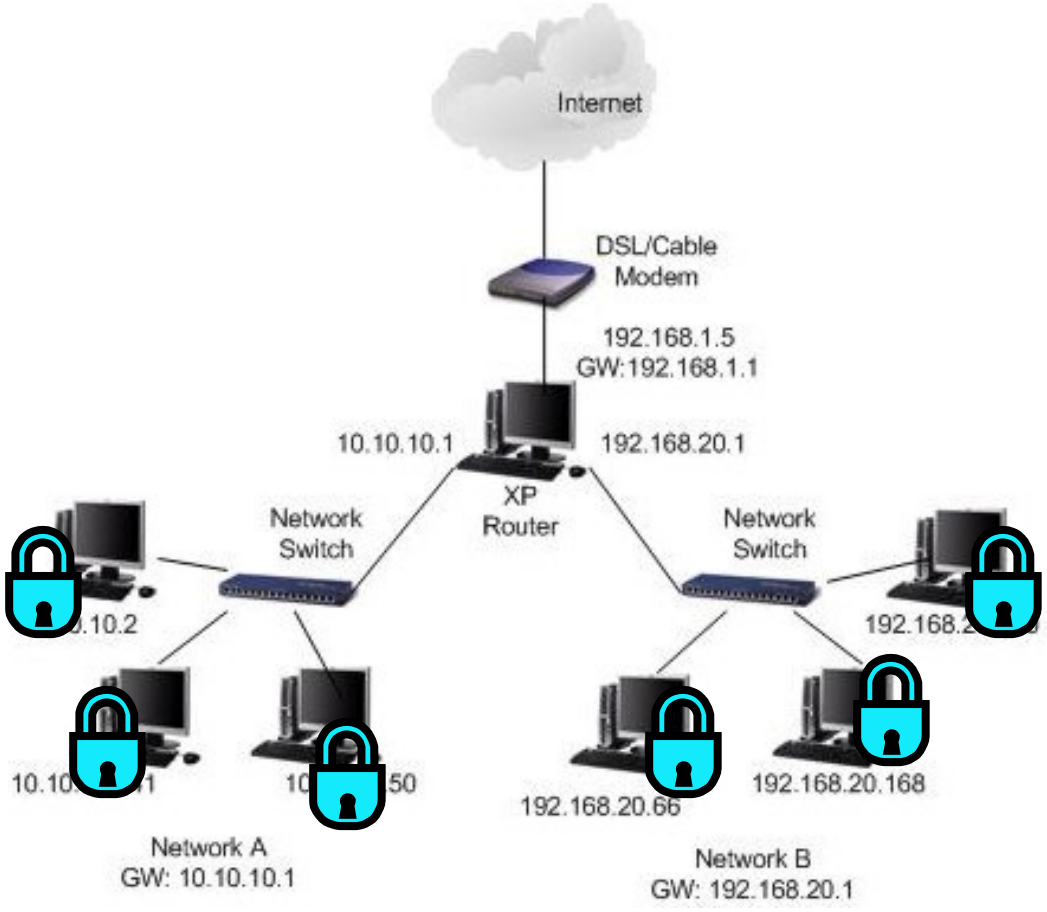
Védelmi rendszerek

CHECKVIR

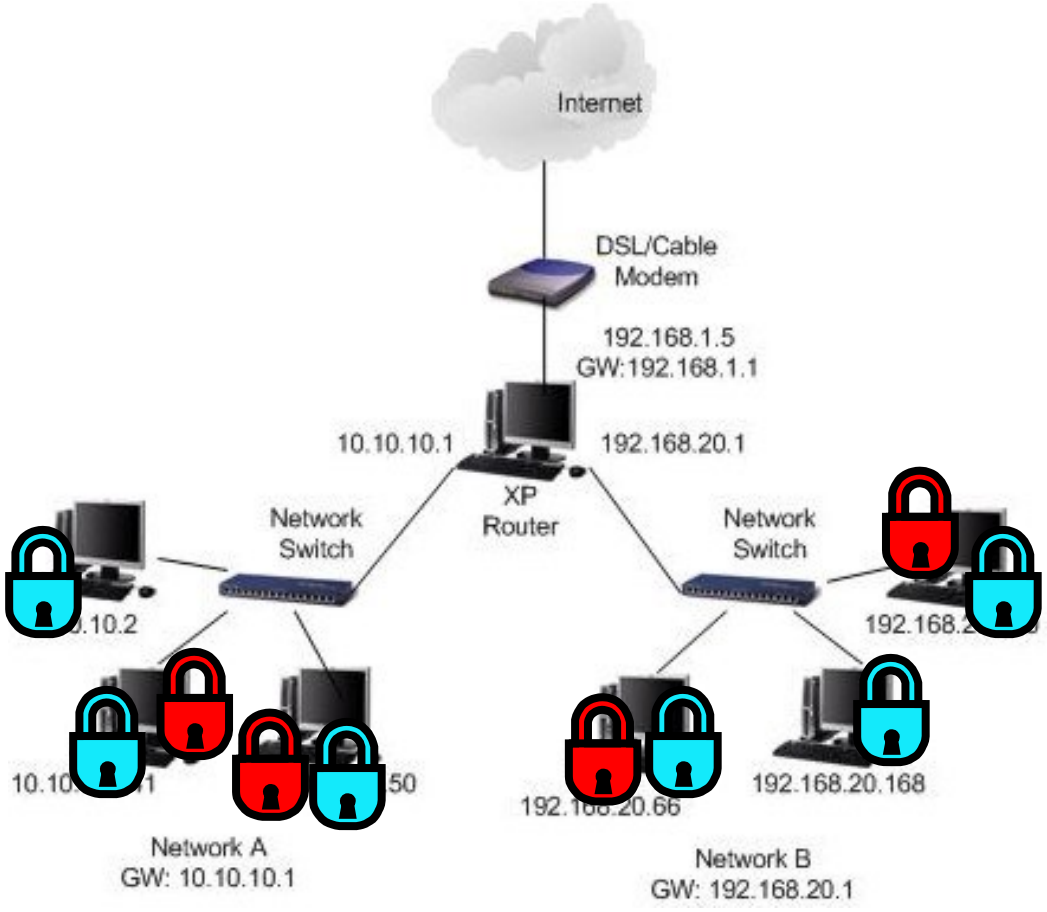
Védelmi rendszerek



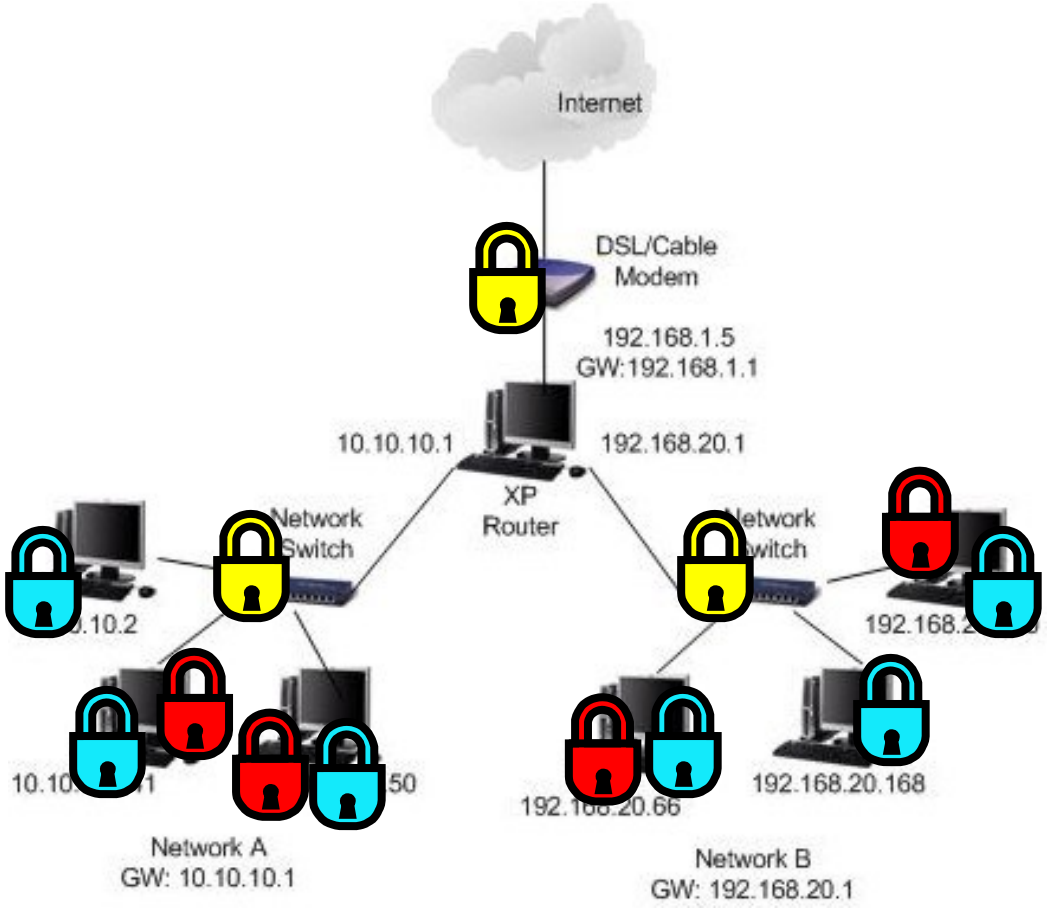
Védelmi rendszerek



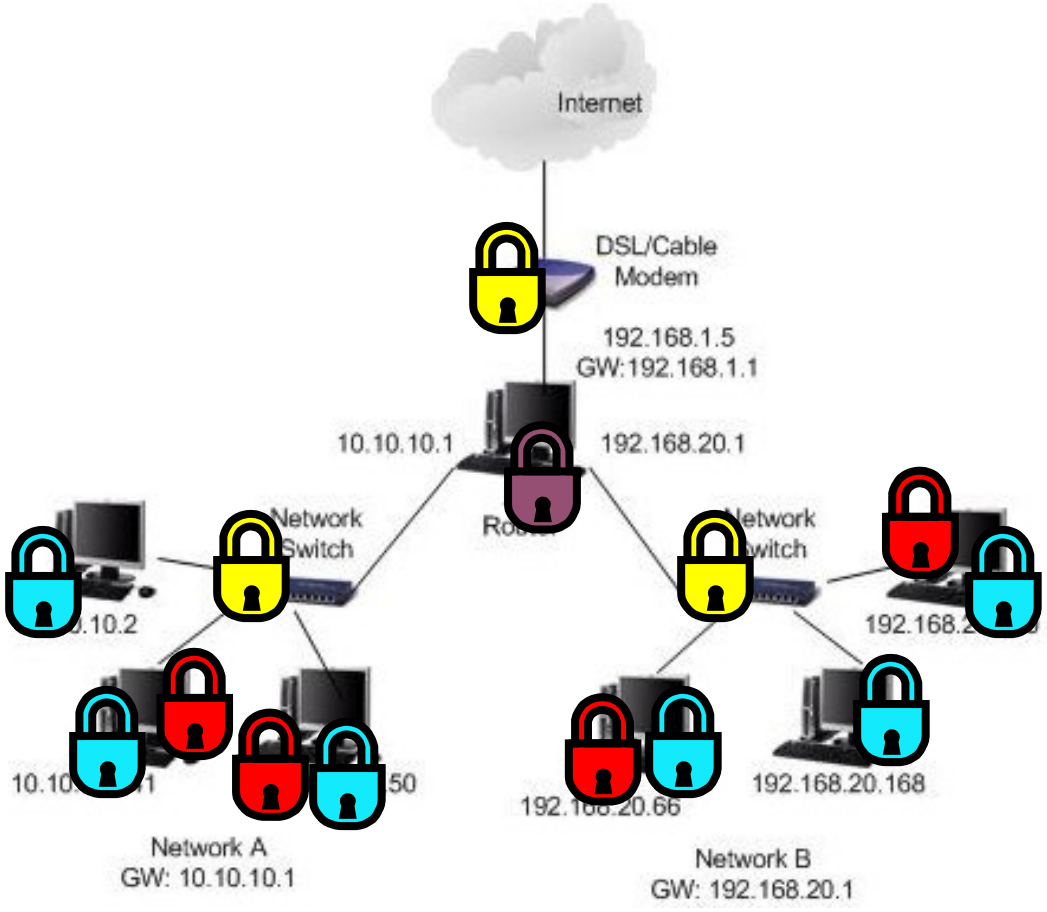
Védelmi rendszerek



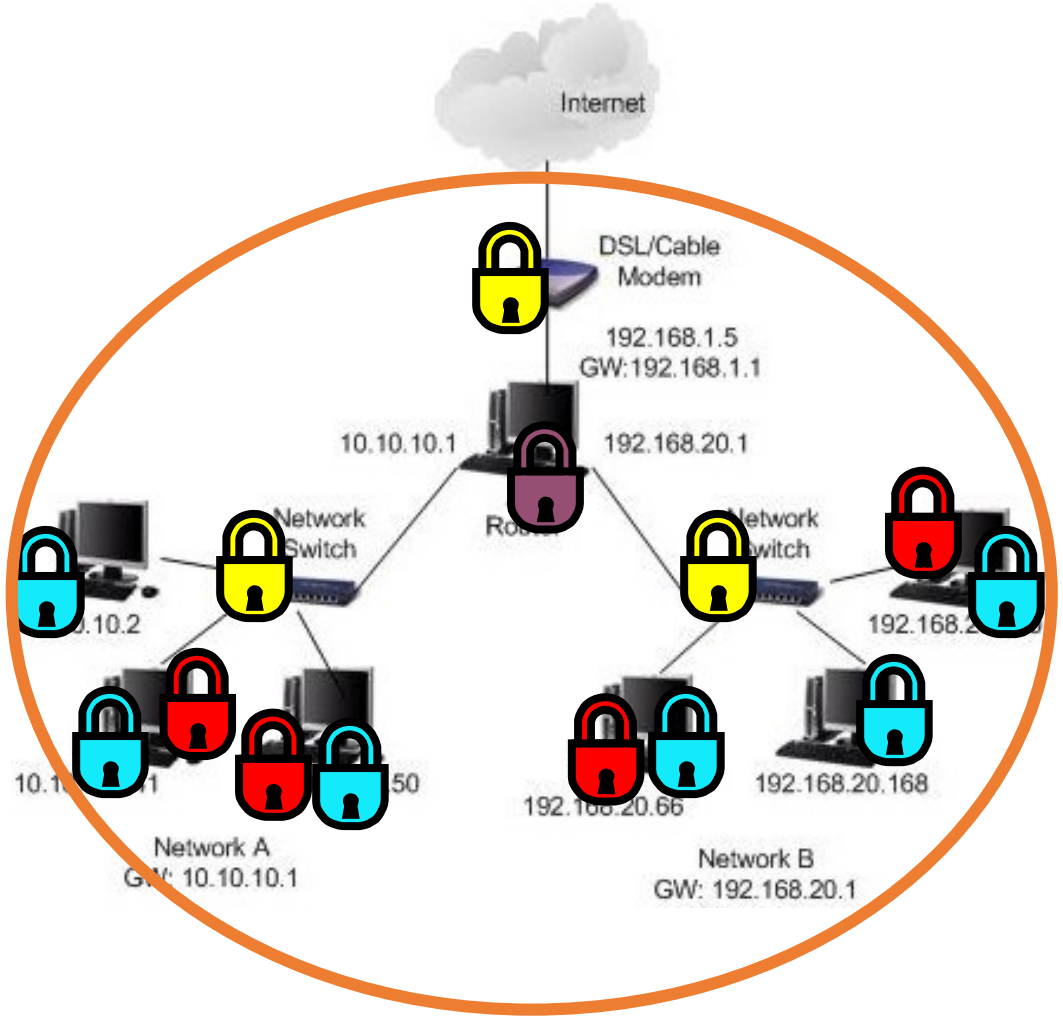
Védelmi rendszerek

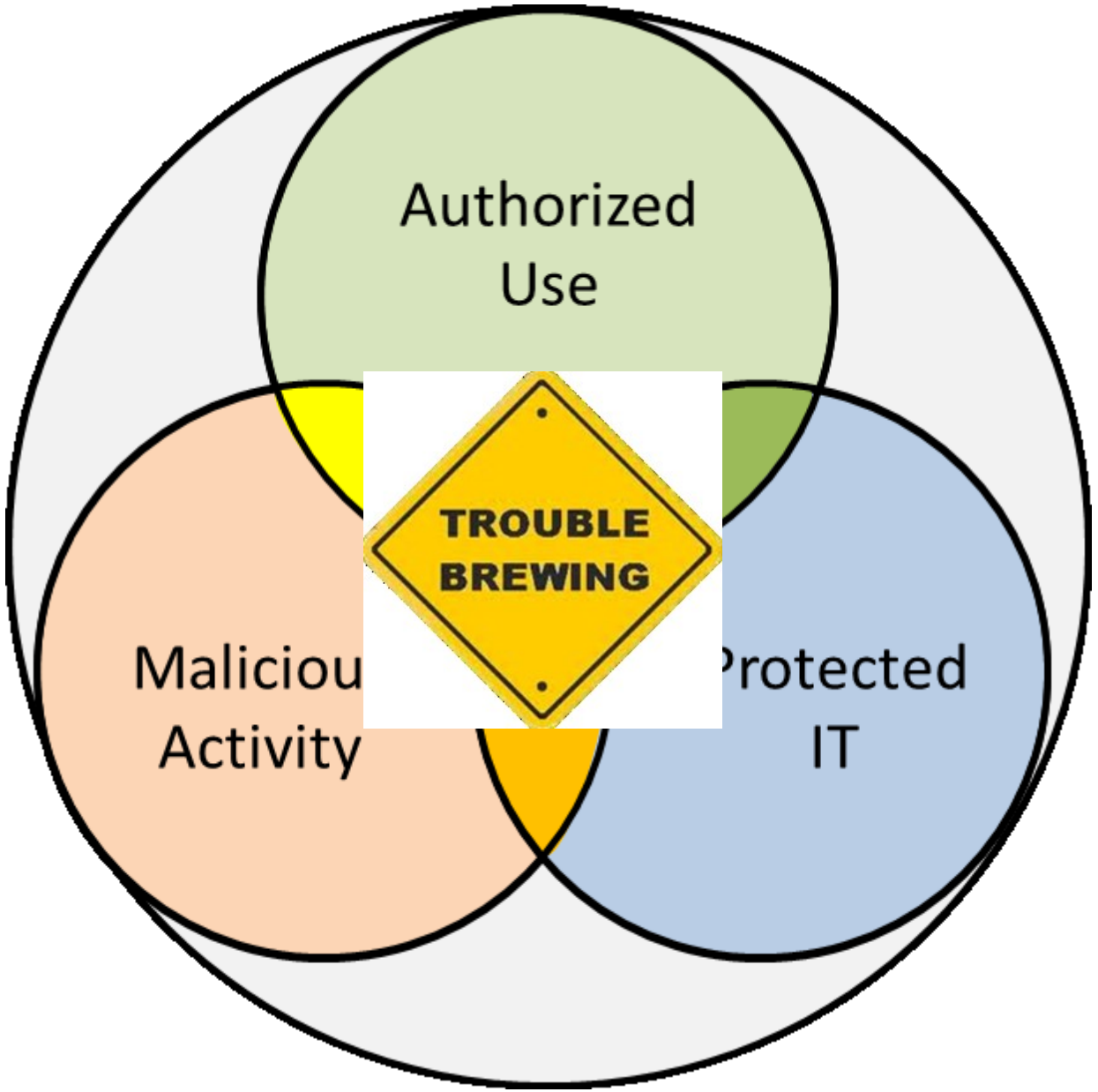


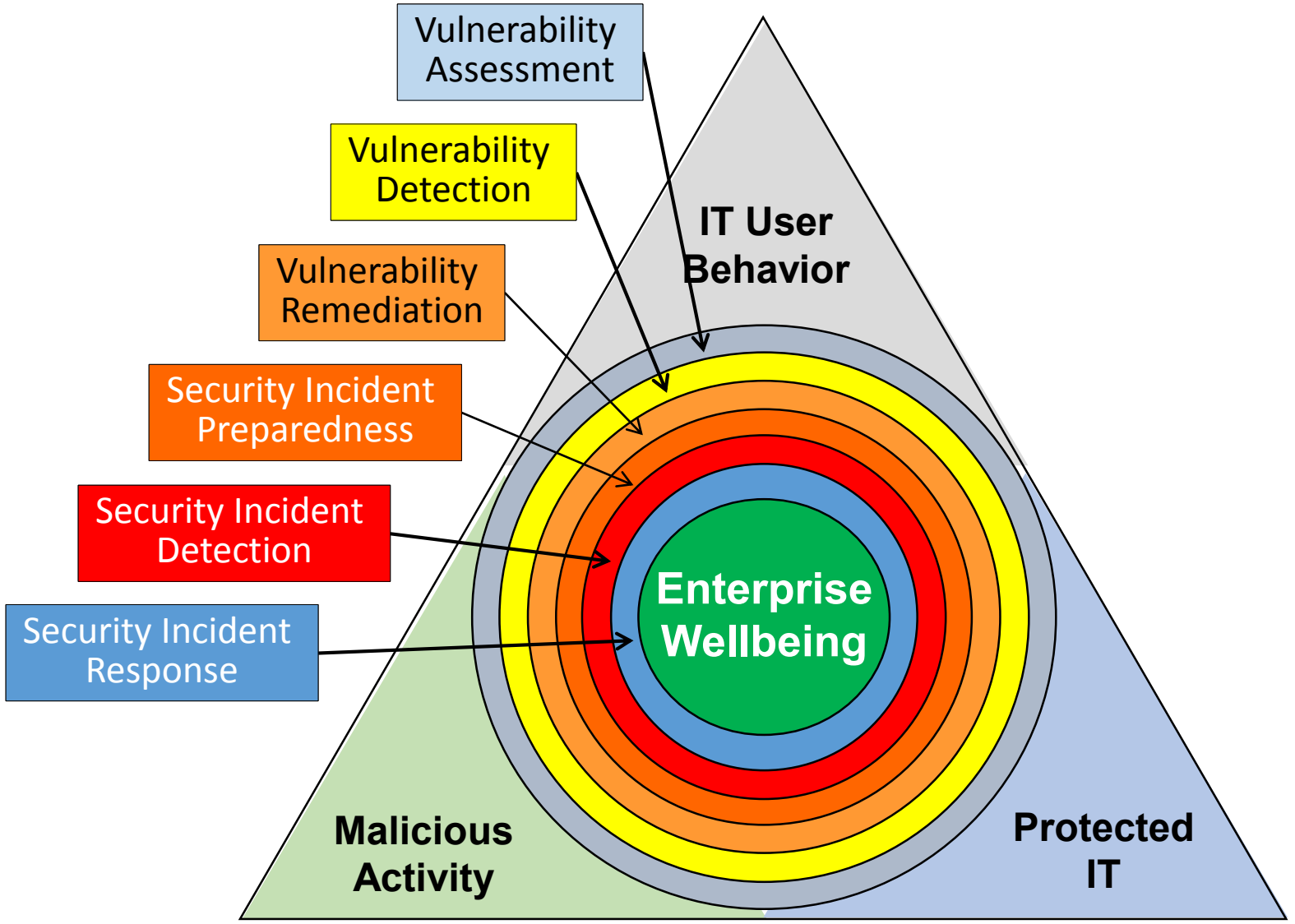
Védelmi rendszerek



Védelmi rendszerek




Authorized
Use
TROUBLE
BREWING
Maliciou
Activity
Protected
IT


Vulnerability Assessment
Vulnerability Detection
Vulnerability Remediation
Security Incident Preparedness
Security Incident Detection
Security Incident Response
IT User Behavior
Enterprise Wellbeing
Malicious Activity
Protected IT

CHECKVIR

Köszönöm a figyelmet!