Security Intelligence.
Think Integrated.

Fenyegetések és válaszok: az IT biztonság kihivásai

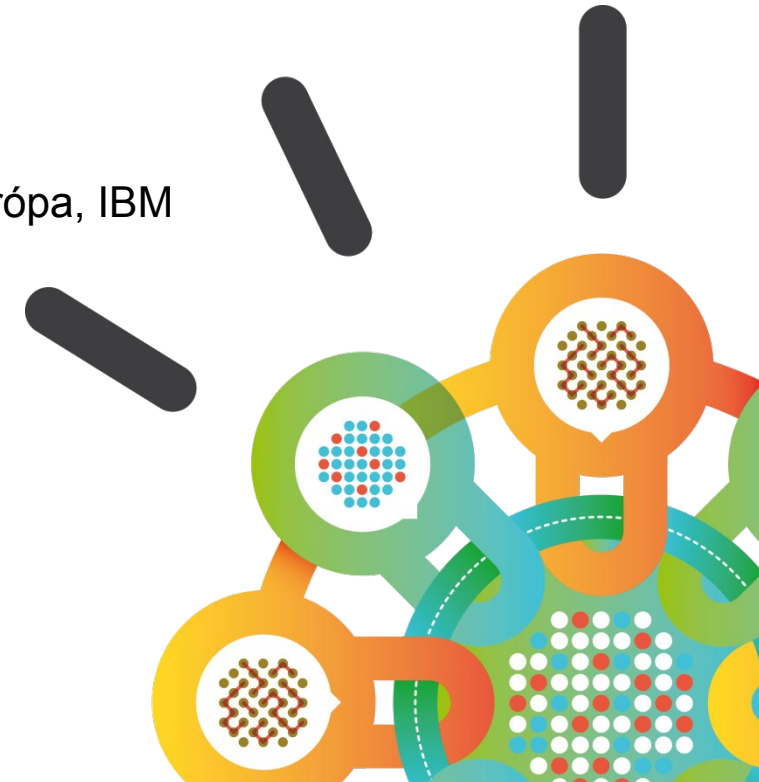
Intelligence, Integration and Expertise

Kocsis Zsolt

Tivoli és ISS szoftver műszaki igazgató, Kelet-Közép Európa, IBM

zsolt.kocsis@hu.ibm.com

2012 Június.12



A világ egyre inkább digitalizált, hálózatba kapcsolt, ami új fenyegetettségeknek nyit ajtót..

Adatrobbanás

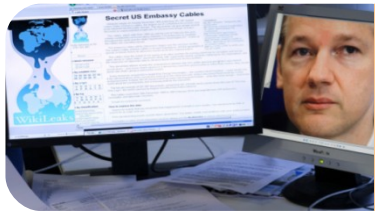
A nagy adatrobbanás korszaka megérkezett, Az alkalmazások a végponti eszközök széles választékáról, bárhonnak elérhetők.

Az IT fogyasztási cikké válik

A választóvonal a személyes és hivatalos adatok, eszközök, alkalmazások és idő között eltűnt.

MInden, mindenhol

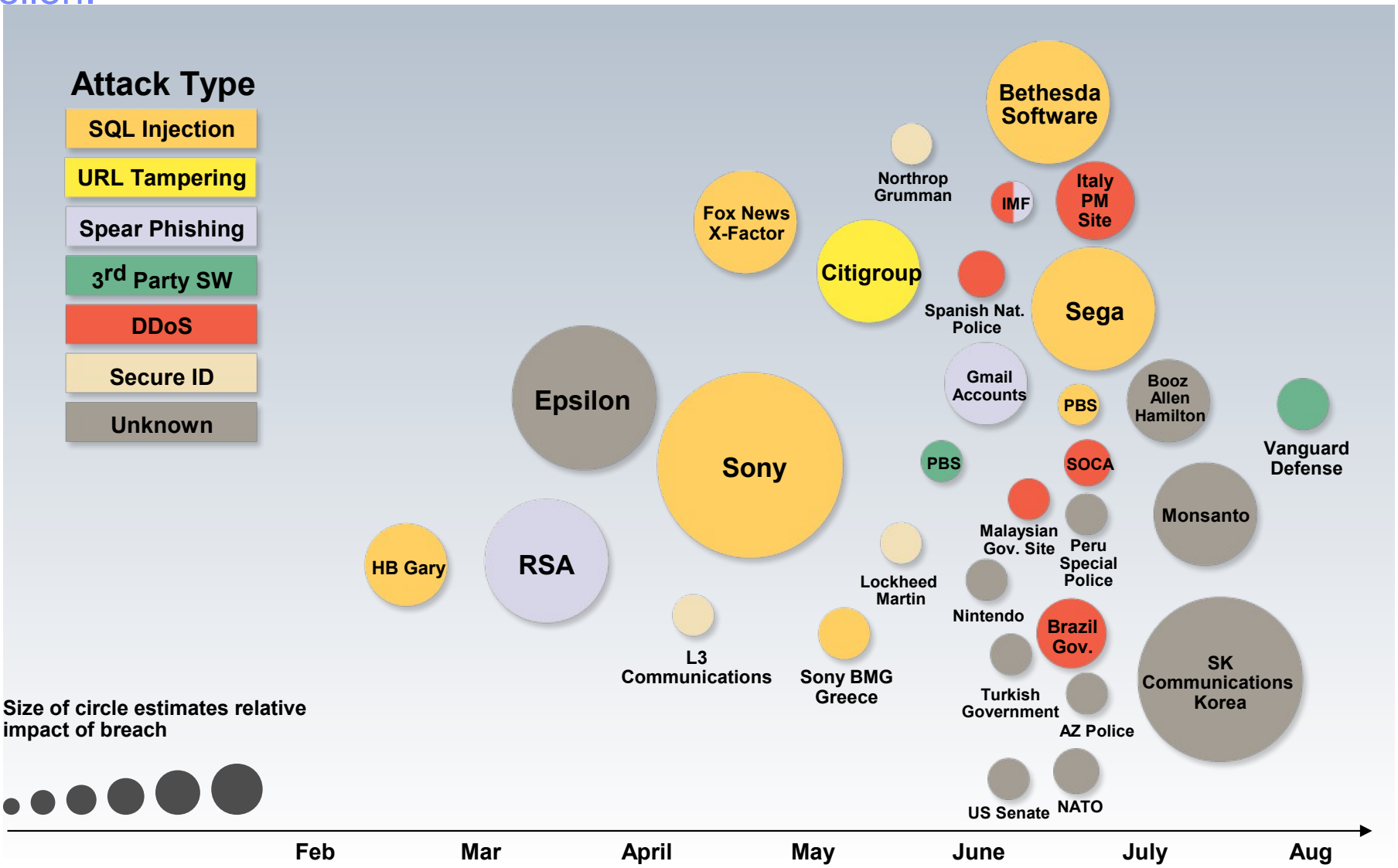
A szervezetek új platformok: felhő, virtualizáció, mobil , web2,közösségi háló alkalmazások irányába nyitnak.



A támadások kifinomultabbá válnak

A támadások sebessége és kiforrottsága megnövekedett, új elkövetők és motivációk jelennek meg: a cyber bűnözéstől a terroristákig, vagy egyes államok által támogatott hacker csoportokig.

2011: Célzott informatikai támadások üzleti és kormányzati célok ellen.



Az informatikai biztonság ügye a cégvezetés asztalára került

Üzleti eredmények	Brand imázs	Beszállítói lánc	Jogi kitettség	Hacktivisták támadása	Audit kockázatok
Sony becslései szerint 1 Miliárd dollár hosszútávú veszteslége keletkezett.	HSBC adatlopás 24 ezer privát banki ügyfelet érintett	Epsilon adatlopás 100 vezető amerikai cég mareting infomációját érintette.	TJX 150M dollár értékű veszteséget okozott a 45M hitelkártya adat ellopása.	Lulzsec 50 napos hack-at-will támadása :Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …	Zurich Insurance büntetése £2.275M ($3.8M) 45 ezer ügyféladat elvesztése miatt.

*Sources for all breaches shown in speaker notes

Kik a támadók?

Támadók és technikák 2011-ben

Off-the-Shelf tools and techniques

Sophisticated

•Válogatás nélküli támadások
•Kifinomult technikai képességek hiánya
•Szokásos hacker eszközök használata
•Robot hálózat építők
•Pénzügyileg motivált tevékennség
•Spam ls DoS támadások

•Cyberwar

Broad

•Pénzügyileg motivált , célzott támadások
•DDOS támadások
•Hacktivisták

•Képzett, folyamatos támadások
•Szervezett, államilag támogatott ssoportok
•Új, Zero day sérülékenységek kihasználása
•Korábban nem használt támadási technikák

Targeted

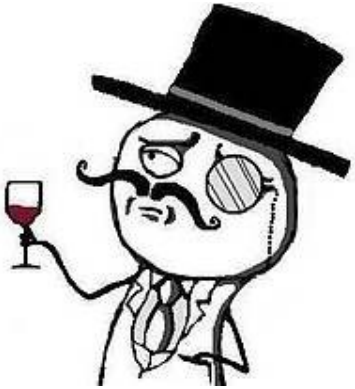
Source: IBM X-Force® Research and Development

Hacktivisták: politikailag motivált IT támadást végző csoportok

A member of Anonymous at the Occupy Wall Street protest in New York*

ANONYMOUS

“We are Anonymous. We are Legion.
We do not forgive.
We do not forget. Expect us.”**



Lulz Security logo

"The world's leaders in high-quality
entertainment at your expense."

*Source: David Shankbone

**Source: Yale Law and Technology, November 9, 2009

A közösségi háló többé már nem csak mellékes szórakozás

A támadók a közösségi hálók adatainak bányászatával képesek szervezetekre, alkalmazottaikra vonatkozó információk megszerzésére.

- Üzleti weboldalak szkennelése, Google, Google news
  - Ki dolgozik ott? Milyen beosztásban?
- Search Linkedin, Facebook, Twitter profilokban
  - Családi kapcsolatok,állatok nevei, címek, dátumok- potenciális jelszavak
  - Kik a kollégáik?
  - Elkezdhető a szervezeti felépítés vizsgálata
- Ki dolgozik az megszerzendő információval?
  - Mi a szervezeti hierarchia, függőségi viszony?
  - Ki a barátaik?
  - Mi az érdeklődési körük?
  - Mi az üzleti / privát email címük, és a barátaiké?
- **Célzott Pfishing támadás indítása**

A kockázatok kezelése és az auditképesség biztosítása egyre összetettebb feladat

Belső fenyegetettség

A privilegizált felhasználók okozzák a belső biztonsági incidensek 87%-át. A belső felhasználók visszaélései által okozott kár az USA-ban évente 600 Milliárd USD.

Nincs központosított biztonsági rendszer

A különböző hálózati és szerver biztonsági megoldások felügyelete összetett feladat.

Külső fenyegetettség

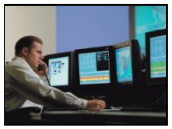
A ismert sérülékenységek 70% ára még nincs kész, megfelelő javítás.

Jogi előírások

Ha jogszabályi megfelelőség nem biztosított,ez pénzügyi, jogi következményeket jelenthet, és a cég jó hírét veszélyeztetheti.

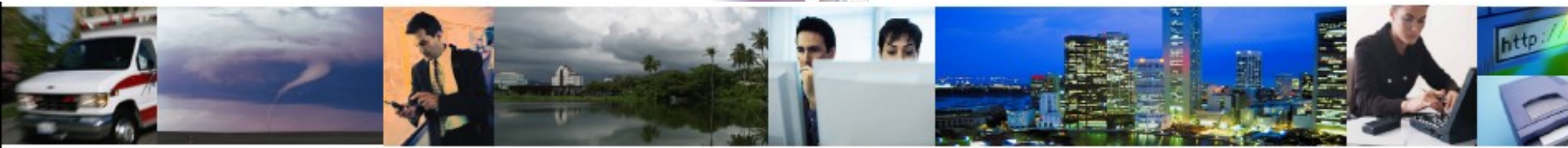
A naplófájl menedzsment idő és erőforrás igényes

A cégek több mint 75% -ának nincs automatizált napló és audit megfelelőség biztosító megoldása.



Üzemeltetés

Túl sok adat, túl sok formátum, túl sok eszköz.



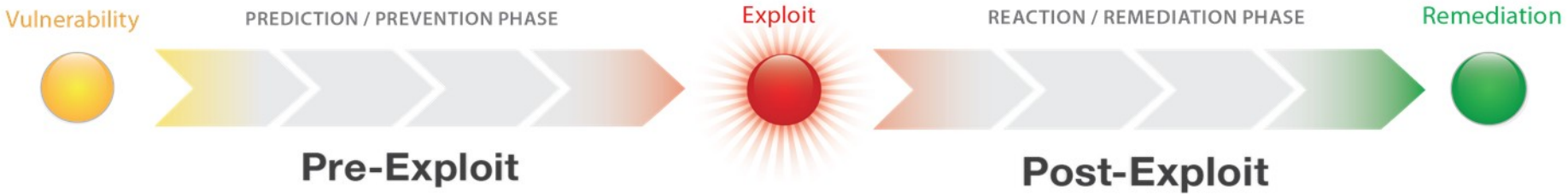
A fenyegetettség fázisai: Milyen megoldást mikor kell használni?

Mik a külső és belső fenyegetettségek?

Képesek vagyunk ezek kezelésére?

Mi történik most?

Mi ennek a hatása?



Előrejelzés és megelőzés

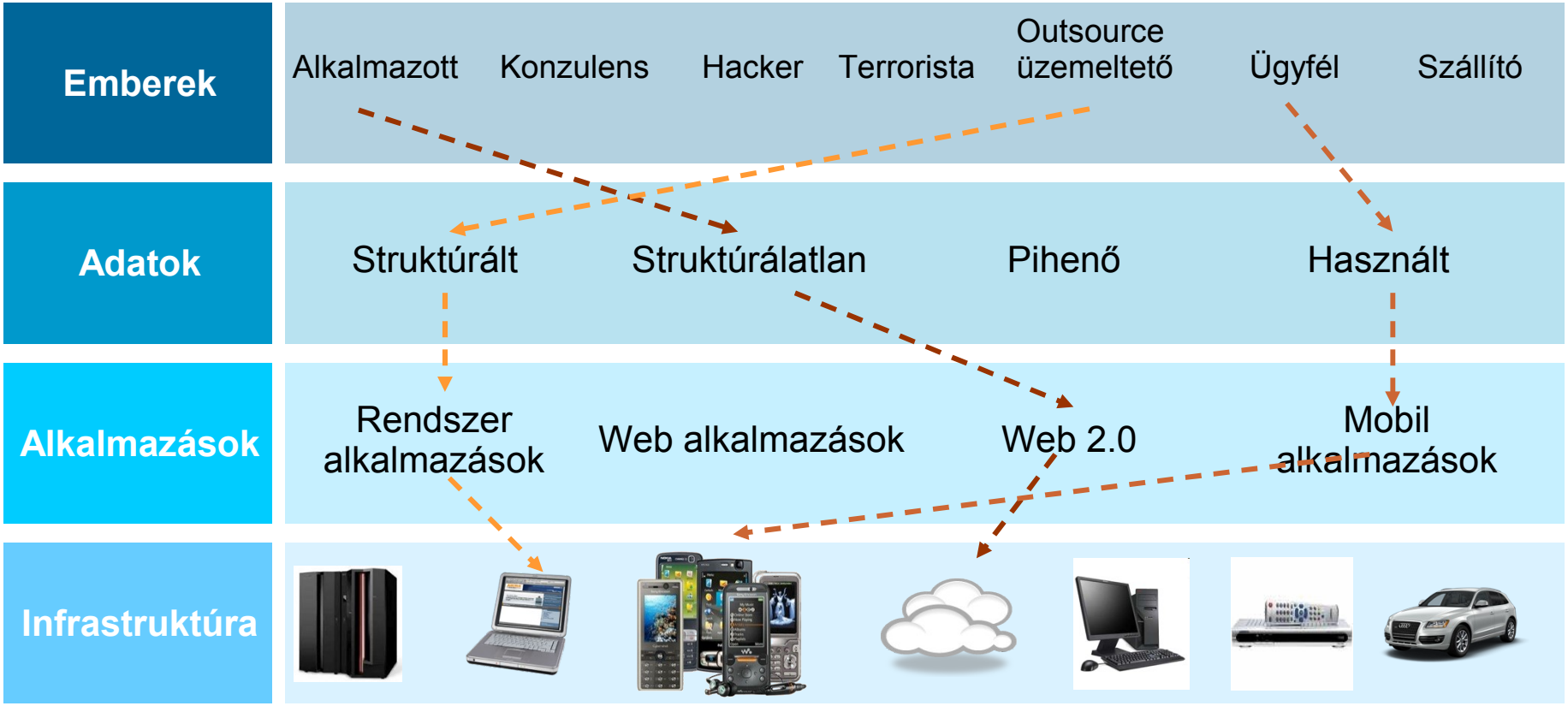
Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Reakció és a hibajavítás

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
SIEM. Log Management. Incident Response.

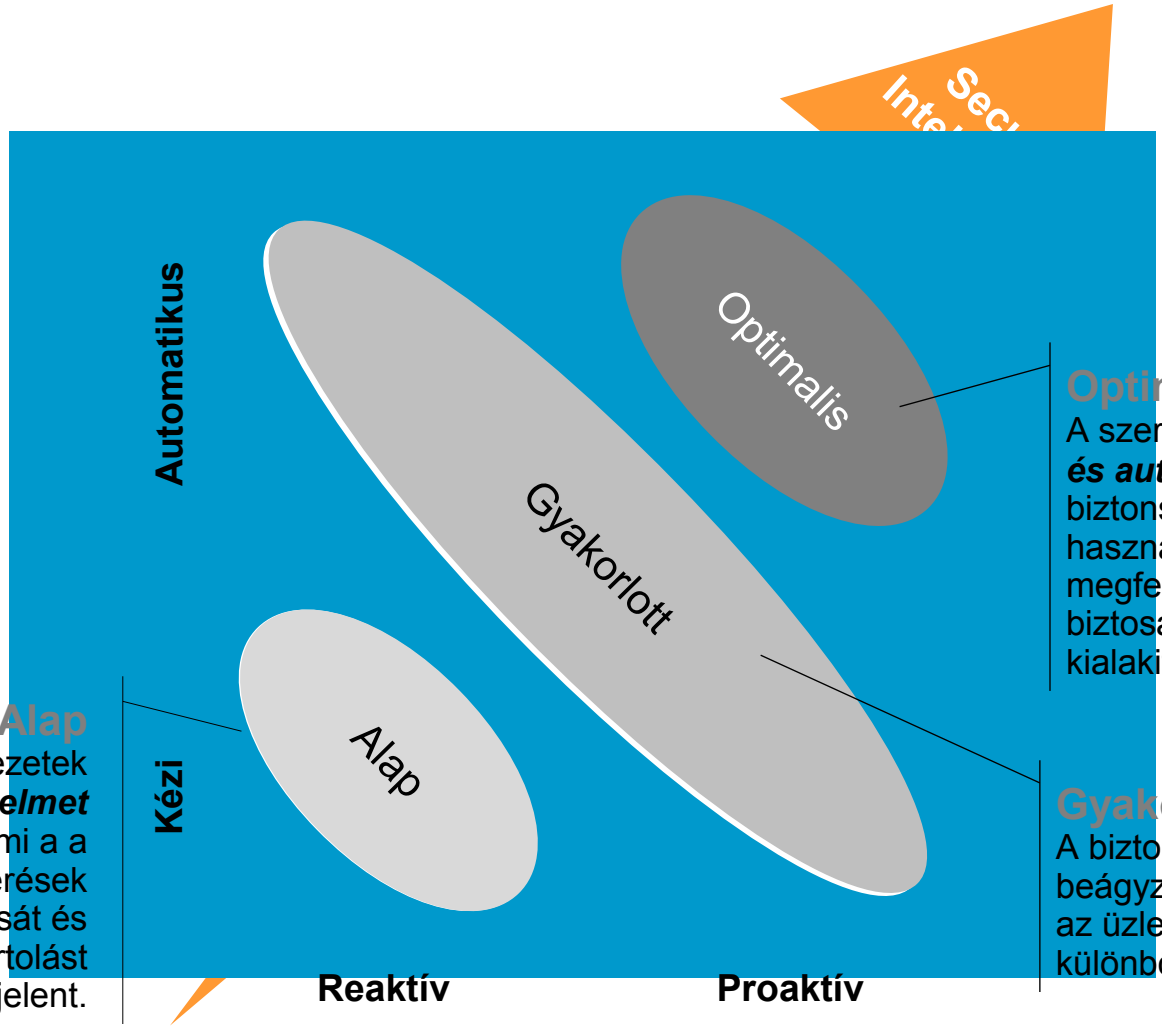
IBM Security Intelligence

Egy biztonsági probléma megoldása komplex, 4 dimenziós kirakó



Nem elegendő csak a határok védelme –
az egyes területeket önállóan lefedő megoldások nem képesek a teljes vállalati biztonságot megteremteni.

Milyen a cégek biztonság-üzemeltetési gyakorlata



Alap
A szervezetek ***perimeter védelmet*** használnak, ami a a hozzáférések szabályozását és manuális riportolást jelent.

Optimális
A szervezetek ***prediktív és automatikus*** biztonsági analitikát használnak, hogy megfeleljenek a biztosági intelligencia kialakításának.

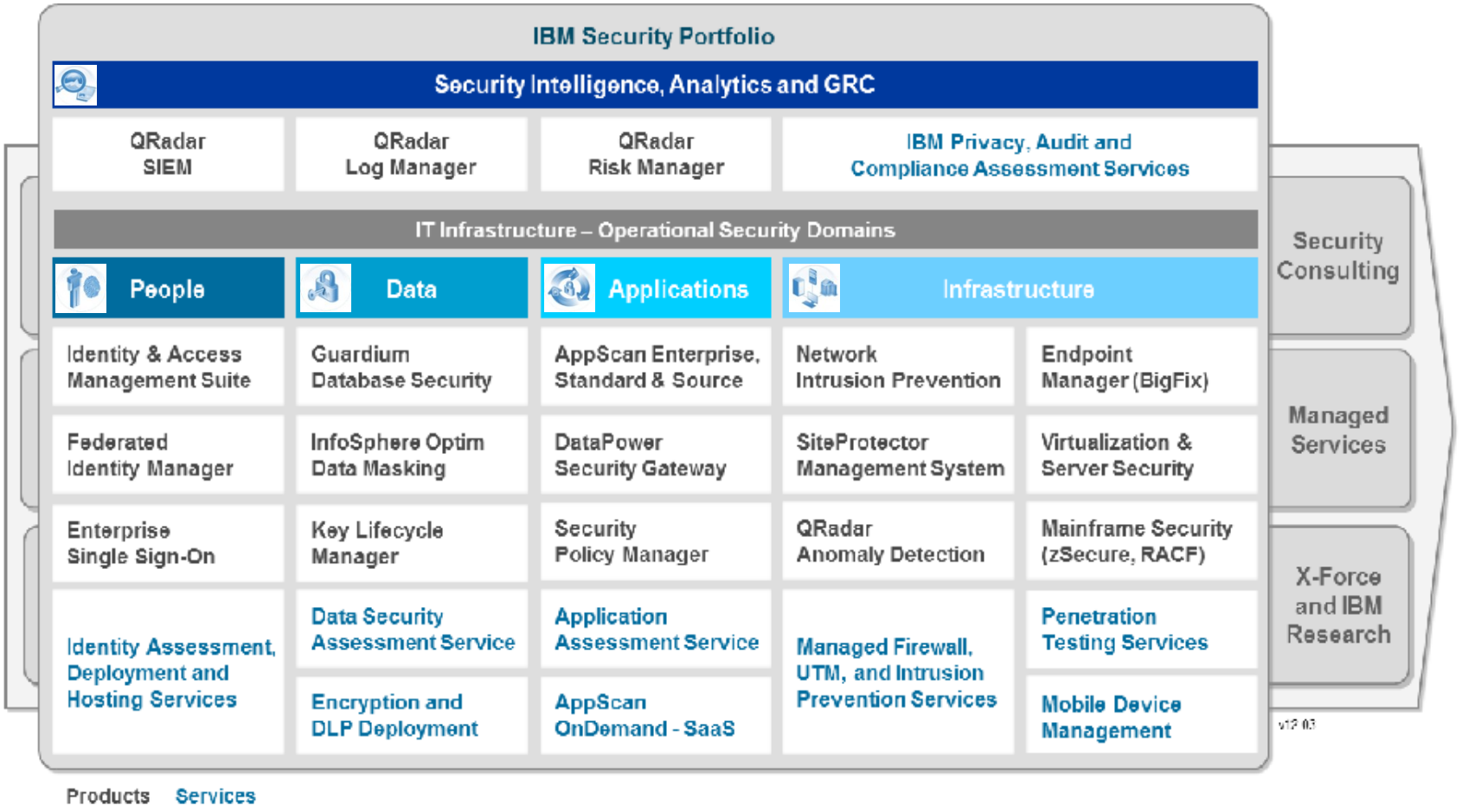
Gyakorlott
A biztonság beágyzódik az IT és az üzleti üzemeltetés különböző rétegeibe.

Security intelligencia lehetővé teszi az optimális szint elérését

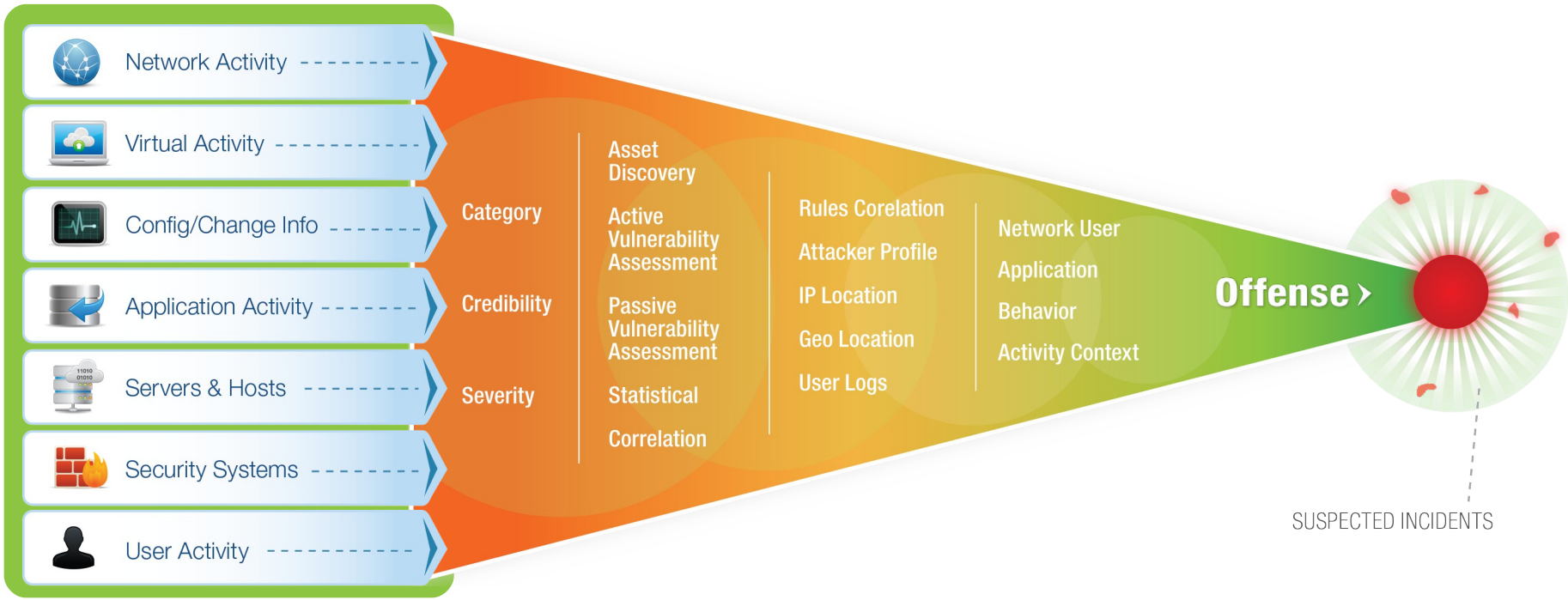
Security intelligencia:
Információ és esemény menedzsment
Magas szintű korrelációs és analitikai technikák
Külső fenyegetettségek kutatása

	Emberek	Adatok	Alkalmazások	Infrastruktúra
Optimális	Szerep alapú analitika Identitás szabályozás Kiemelt felhasználók tevékenység kontrollja	Adat áramlás kontroll Adat szabályozás	BIztonságos alkalmazás fejlesztési módszertanok Csalás érzékelés	Inteligens Hálózat monitorozás Forensics / adatbányászat Biztonságos rendszerek
Gyakorlott	Jogosultság ellátás Hozzáférés mgmt Erős authentikáció	Hozzáférés monitorozás Adatvesztés megelőzés	Alkalmazás tűzfal Forrás kódok szkennelése	Virtualizáció security Eszköz mgmt Végpont / hálózat biztonság menedzsment
Alap	Központi címtár	Titkosítás Hozzáférés kontroll	Alkalmazások szkennelése	Perimeter biztonság Anti-virus

Az IBM Security Systems megoldás portfóliója

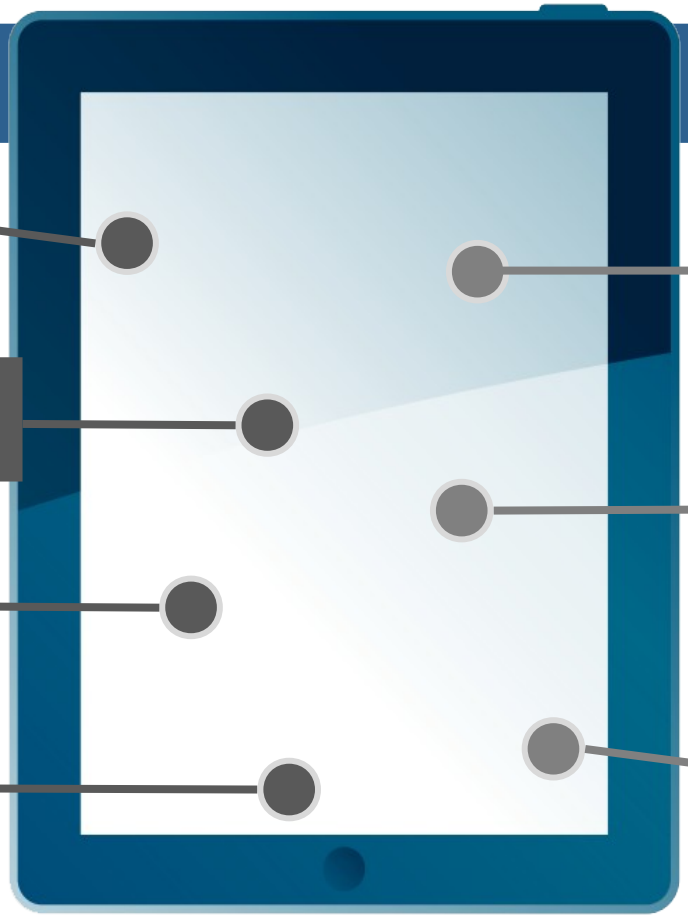


Az IBM integrálja a különböző forrásokból származó eseményeket, adatokat



Átfogó források + Intelligencia = Pontos és végrehajtható eredmények.

Az mobil eszközök elterjedésével az informatika fogyasztási cikké vált, széleskörűen elérhető és támadásra használható.



IBM Mobil Security szoftverek

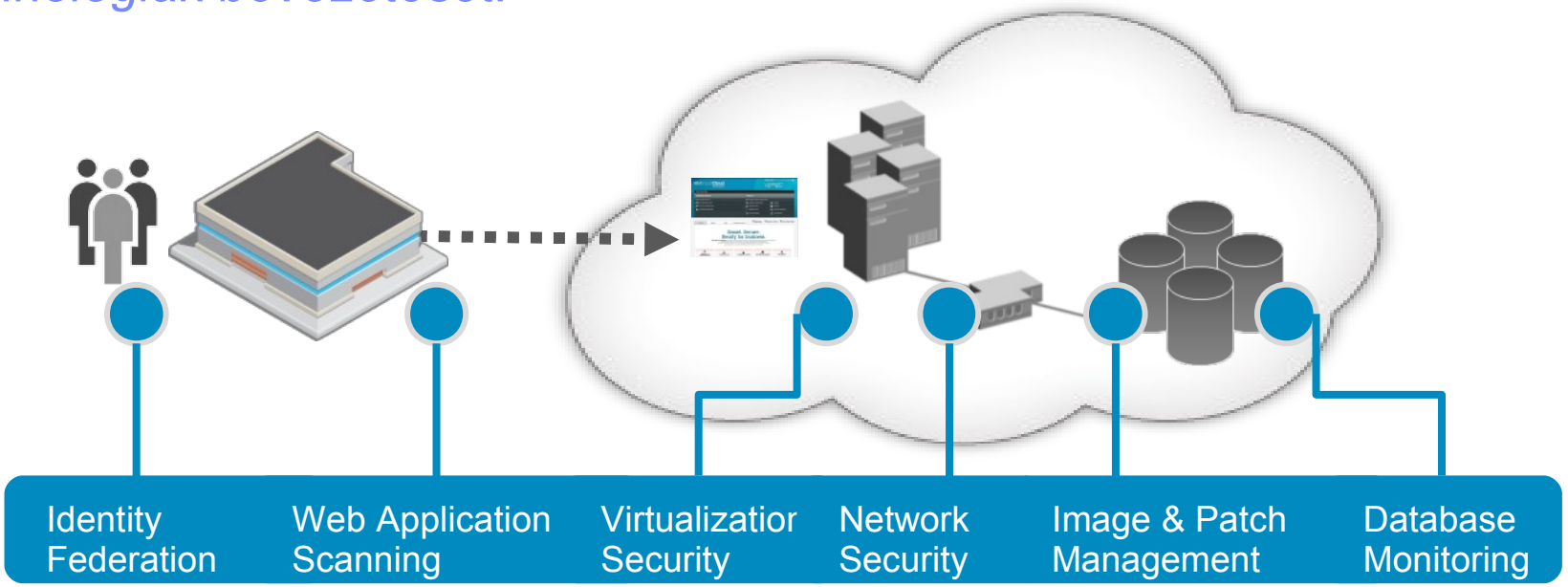
- Eszköz leltár
- Biztonsági házirend menedzsment
- Eszköz és adat törlés
- Anti-Jailbreak Anti-Root

IBM Mobil Security szolgáltatások

- **Életciklus menedzsment** Mobile Enterprise Services (MES)
- **Végpont menedzsment** Hosted Mobile Device Security Management
- **Biztonságos kapcsolódás** Secure Enterprise Smartphone and Tablets

Minden, mindenhol a felhőben is.

IBM elosztott, többszintű biztonsági megoldásai támogatják a felhő alapú technológiák bevezetését.



IBM Security Intelligence

A biztonság nem (csak) technikai probléma, hanem üzleti kihívás

A 2011 év adatlopásai közül számos megelőzhető lett volna,de

- Jelentős erőforrásokat igényel a sérülékenységek megtalálása, beazonosítása és lezárása.
- A pénzügyi és operatív ellenállás jellemző: mekkora invesztíció lenne szükséges és elegendő a probléma kezelésére?

Mia legfontosabb 10 javaslatunk?

1. Rendszeres, külső cég által végzett biztonsági audit.
2. A végpontok felügyelete.
3. Érzékeny rendszerek és adatok szegmentálása, és ennek megfelelő védelmi házirendek, eszközök alkalmazása.
4. A hálózati réteg védelme, automatikus eszközök segítségével.
5. Web alkalmazások auditálása
6. Az alkalmazottak oktatása adathalászati támadások kivédésére.
7. Megfelelő jelszó politika, hozzáférési és jogosultság kezelési megoldások használata.
8. Minden projekt terv tartalmazza annak biztonsági vonatkozásait is.
9. Az üzleti partnerek adatkezelési gyakorlatát is meg kell vizsgálni.
10. Legyen szilárd és kipróbált incidens elhárítási tervünk.

Az IBM globális biztonsági kutatási, fejlesztési és szolgáltatási szervezete

IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

14 Milliárd elemzett weboldal

40M spam & phishing támadás

54K dokumentált sérülékenység

Több milliárd behatolási kísérlet elhárítása naponta.

Malware minták milliói

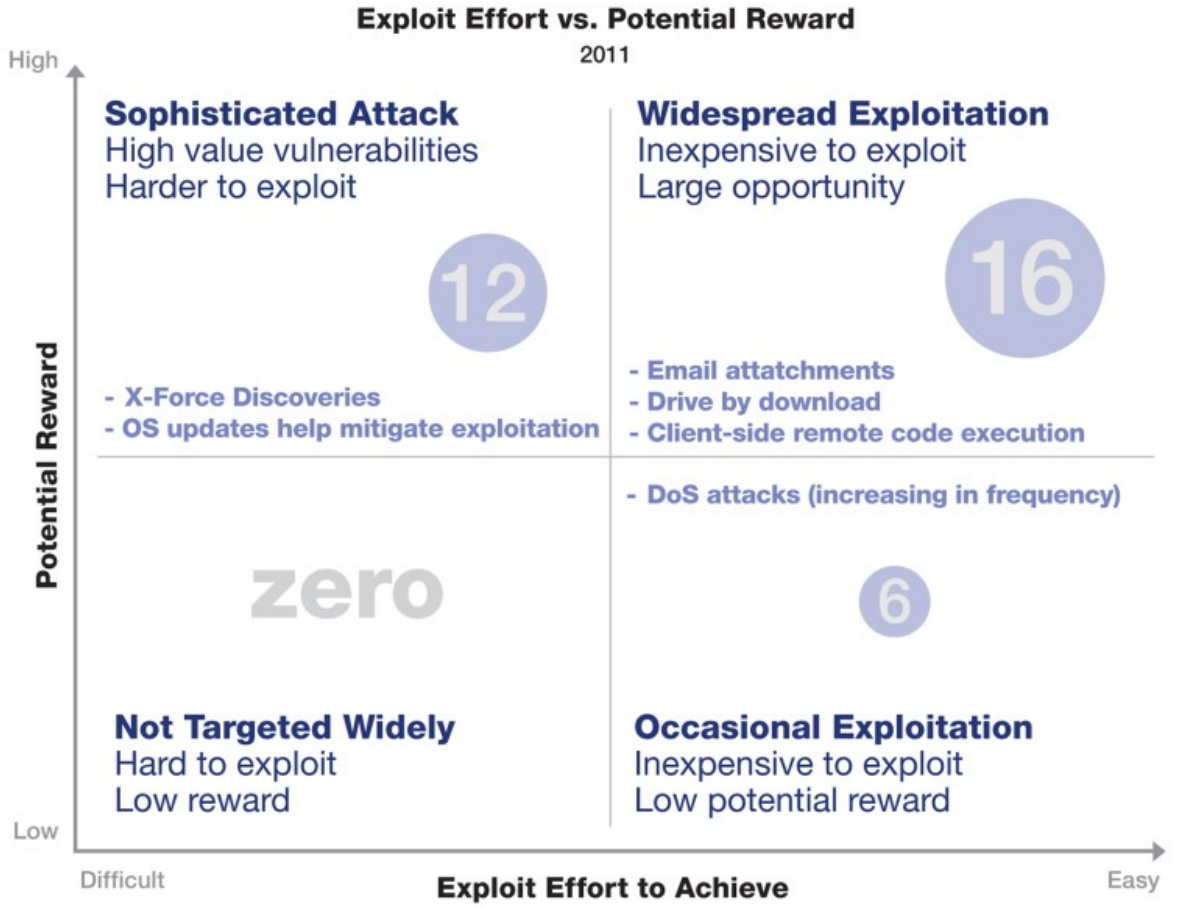
X-FORCE

World Wide Managed Security Services

- 20,000+ védett eszköz
- 3,700+ MSS ügyfél
- 13Mrd+ menedzselt esemény naponta
- 1,000+ biztonsági szabadalom
- 133 országban érhető el(MSS)

Legfontosabb X-Force riasztások: 2011-ben.

- 34 globális X-Force riasztás és bejelentés 2011-ben:
  - 16 kritikus riasztás
  - Könnyen kihasználható sérülékenység, nagy károkozási potenciállal
  - 12 nehezebben kihasználható, de nagy kárt okozó sérülékenység.



Source: IBM X-Force® Research and Development

Hol éri el az IBM X-Force biztonsági kutató részlegének eredményeit.

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports

http://www.ibm.com/security/xforce

Subscribe to X-Force alerts at http://iss.net/rss.php or Frequency X at http://blogs.iss.net/rss.php

Attend in-person events

http://www.ibm.com/events/calendar/

Join the Institute for Advanced Security

www.instituteforadvancedsecurity.com

Subscribe to the security channel for latest security videos

www.youtube.com/ibmsecuritysolutions

Köszönöm figyelmüket.

ibm.com/security