Veszélyes felhasználói akciók megelőzése

- úttörő technológia a tevékenység felügyeletben-

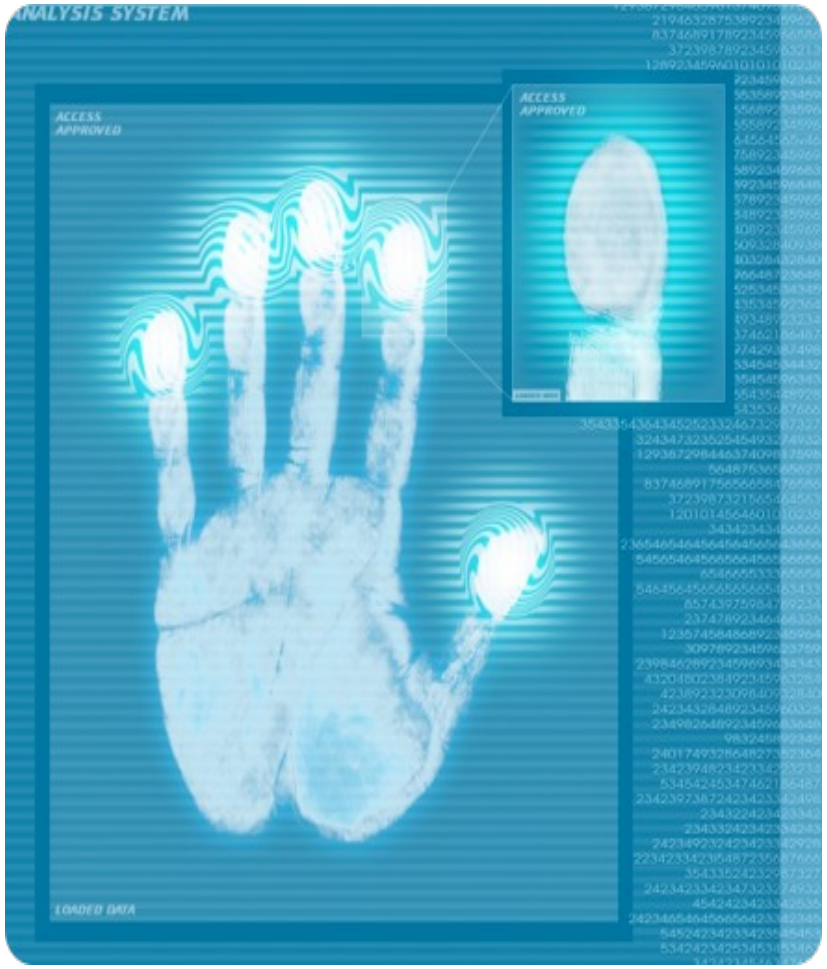
Miről lesz szó

- Kiemelt felhasználók
- Naplózás
- Monitorozás másképpen
- Megelőzés egy új technológiával

Múltbéli események

Privilégizált felhasználók

- Kikről beszélünk?
  - Rendszergazdák
  - Kiemelt felhasználók
  - Fejlesztők
  - ...
- Külsősök – belsősök
- Nem a “normál” irányból érik el a rendszereket



Miért kell őket ellenőrizni?

- Megfelelőség
- Külső kényszer
- Belső szabályozás
- Bizalom hiánya

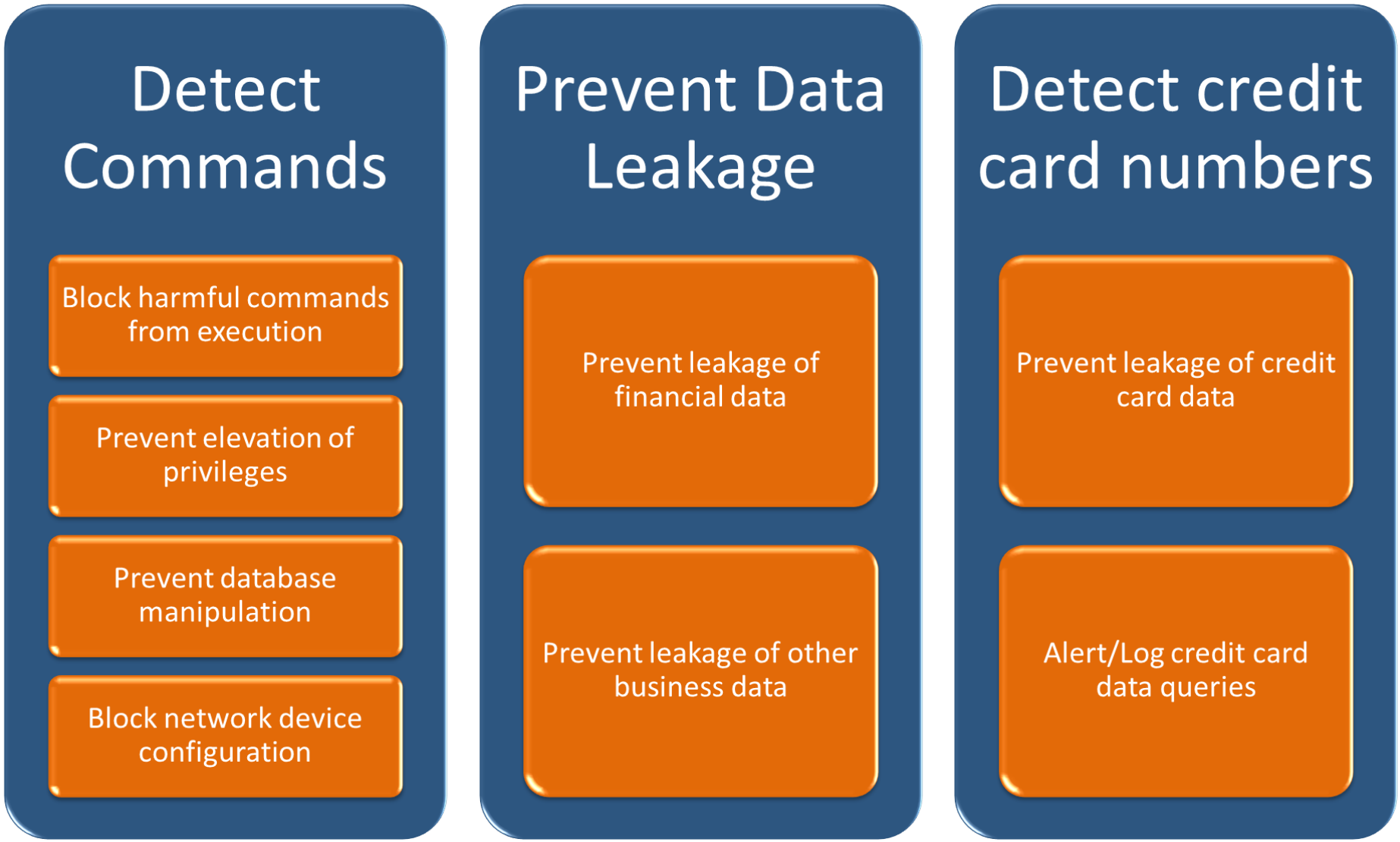
Naplózás

- Bevált módszer események követéséhez és elemzéséhez
- Pár probléma
  - Felhasználói tevékenység nehezen követhető
  - Események részletei elérhetőek-e?
  - Adat-forrás mennyire megbízható?
  - Túl nagy “zaj”

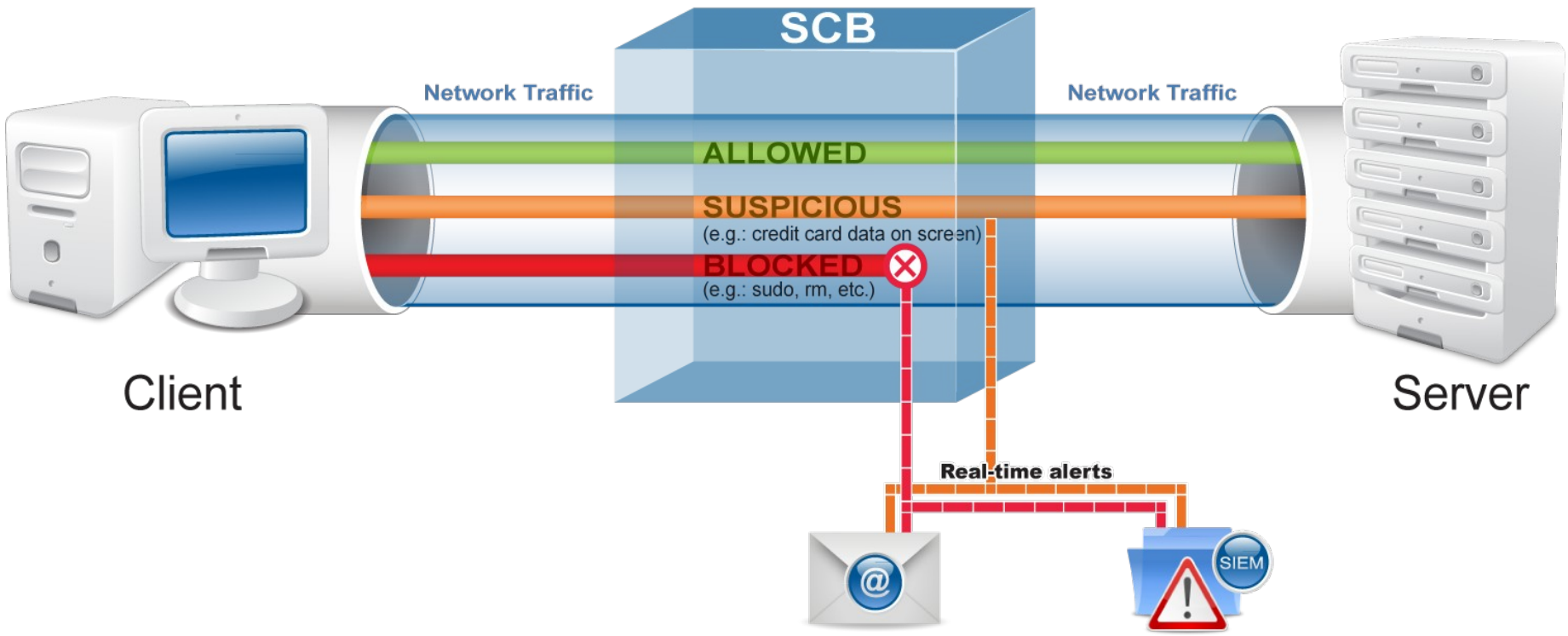
Monitorozás vs. megelőzés

- Monitorozás hasznos, de akkor már megtörtént a baj!
- Nem kívánt esemény sokáig rejtve maradhat
- Nem lehetne valahogy meggátolni az eseményeket?

Meggátolni, de mit?



Hogyan működik?



Real-time alerting and blocking by SCB

Valós idejű elemzés - prevenció

- Felhasználói aktivitás valós-idejű feldolgozása
  - Tiltás – Engedélyezés – Riasztás – Naplózás
- Riasztások és riportok esetében is használt intelligencia alkalmazása az élő munkameneteken
- SSH kapcsolatban kiadott parancsok szűrése
- Riportok mellett azonnali riasztás vagy megelőzés

```
root@server:~$ vi /etc/passwd
root@server:~$ vi /etc/shadow
root@server:~$ /etc/init.d/apache2 stop
 * Stopping web server apache2
root@server:~$ /etc/init.d/syslog-ng stop
 * Stopping system logging syslog-ng
```

SCB: Parancsok szűrésén túl...

- Sokszor nem a rendszer, hanem az adatok védelme a cél!
- Távoli hozzáférésen keresztül elérhető adatok szűrése
  - Adatokhoz történő jogosulatlan hozzáférés tiltása!
- Képernyőn megjelenő bármilyen tartalom ellenőrzése
  - PI: hitelkártya vagy személyes adatok, céges információk
  - Adatszivárgás privilégizált felhasználók esetében

```
root@server:~$ cat credit-card
John Doe MasterCard          5542 0432 0455 9001
Secure Access Code: 5432
root@server:~$
```

DEMÓ

Milyen előnyökkel jár?

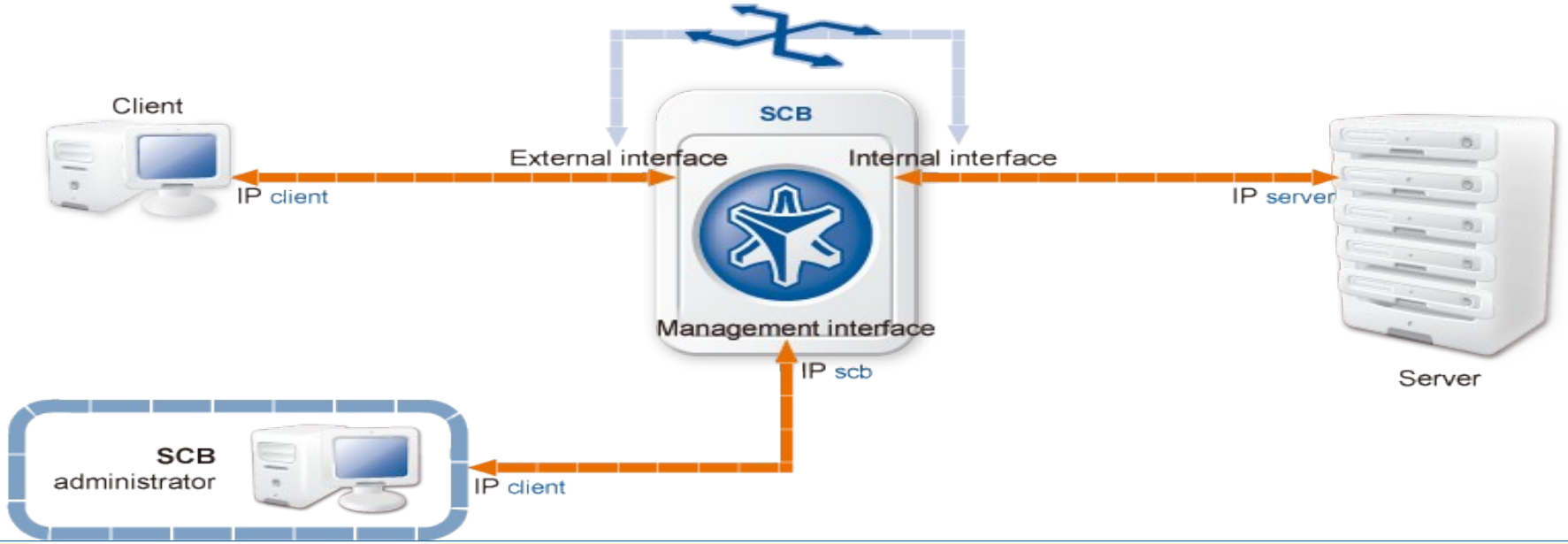
- Valós idejű forgalom elemzés
- Kapcsolat bontás is lehetséges
- Azonnali értesítés
- Utólagos nyomozás helyett megelőzés
- Hitelvesztés megakadályozása

Technológia további lehetőségei

- Grafikus protokollok elemzése:
  MS Terminal Services, Citrix XenApp, VNC, X11
  - Vírtuális képernyő valós idejű építése, elemzése, szövegek felismerése, akciók vágrehajtása
- Intelligencia
  - Nem mindig tudjuk megfogalmazni, hogy mi a káros
  - Intelligencia a gyanús esetek kiszűrésére

Shell Control Box

- Független monitorozó megoldás
- Távoli eszközök hozzáférésének kontrollja
  - SSH, RDP (Terminal Services), Citrix ICA (XenApp, XenDesktop), TELNET, TN3270, X11, VMWare View, HTTP(S)
- Teljes munkamenetek rögzítése
  - Vissza-játszás, keresés, indexelés, riportok



Köszönöm a figyelmet!

Stange Szilárd
BalaBit IT Security