A belső védelmi rendszer megerősítése

SIEM megoldások kiegészítése jogosultsági információkkal, konfigurációkezeléssel és tevékenységfigyeléssel

Hargitai Zsolt
Üzletfejlesztési igazgató
zhargitai@novell.hu

NetIQ®

"Energy company reports $1 billion in charges and a loss" - New York Times

"Security Breach Exposes Data on Millions of Payment Cards" - InformationWeek

Home Depot breach could be as big as Target's – Computerworld

"Bank loses personal data on 248,000 customers"

"Hospital patient data revealed"

Neiman Marcus Sued Over Customer Credit Card Data Breach

- Bloomberg

"Identity Theft Remains a Concern for Bank Customers Amid Economic Slowdown"

– The Wall Street Journal

"Target says up to 70 million more customers were hit by December data breach" – The Washington Post

"ID-theft case leads to mail conviction"

"Health care data breaches have hit 30M patients and counting…" – The Washington Post

A cégek több mint 60%-ának volt legalább egy biztonsági eseménye az elmúlt 12 hónapban.

Frequency of successful attacks in the past 12 months:

More than 10 times	7%
Between 6 & 10 times	9%
Between 1 & 5 times	46%
Not once	38%

2014 CYBERTHREAT DEFENSE REPORT NORTH AMERICA & EUROPE – Cyberedge Group

Túlzott magabiztosság

IT informatikai vezetők szerint a cégük átlagosan **10 hours belül** észleli a biztonsági eseményeket

- 35% szerint perceken belül
- 22% szerint gyakran eltart egy napig
- 5% szerint sokszor eltart egy hétig is

42% nyilatkozott úgy, hogy védettnek érzi a cégét

Vanson Bourne study

A támadást elszenvedett szervezetek között **egy sem volt,** amelyik észlelte volna a támadást **perceken vagy órákon belül.**

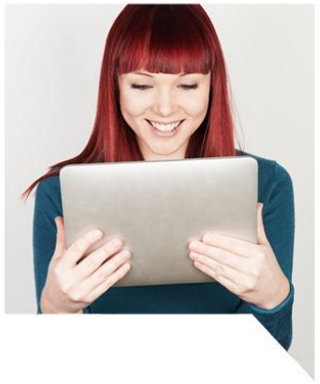
- > 27% néhány napon belül
- 24%-nak hetekig tartott
- 39%-nak hónapokig
- 9%- nak több mint egy évig

2012 Verizon Data Breach Investigations Report

Gyorsan változó környezet

Felhő

Mobilitás



BYOD

Közösségi hálózatok

Otthon ⟷ **Munkahely**

Felhasználók által kezdeményezett változások

A hagyományos megközelítés nem hatékony

Az elmúlt években a kiberbűnözők új, fejlettebb módszerekkel kezdtek el dolgozni

- A peremvédelem feltörése
- A rossz biztonsági gyakorlatok és konfigurációk kihasználása
- Egyre fejlettebb adathalászat
- A szolgáltatók támadása
- Kiemelt felhasználók jogosultságainak kihasználása

“5 of the Top Security Breaches of 2013”
Brian Prince, *SecurityWeek*, January 02, 2014

In no particular order, here are some of the most serious security incidents that made the news in 2013.

1) **Target:** The latest publicized breach of the year was also one of the biggest, affecting as many as 40 million payment cards. According to Target, malware was discovered on some of the chain's point-of-sale systems Dec. 15. Anyone who shopped at a Target store and used a credit or debit card between Nov. 27 and Dec. 15 should stay alert for suspicious activity. Last week, the store also confirmed that encrypted PIN data was removed, though Target believes that information is still safe because the encryption key necessary to decode the PIN information is not stored or accessed by Target. Besides consumers concerns, the breach touched off questions about why Target had not adopted EMV chip technology to better protect its customers.

2) **Adobe Systems**: Adobe was hit hard after news leaked out that attackers had accessed the encrypted credit card information of millions of customers and compromised the account information of millions more. The breach also involved the theft of source code for a number of the company's products, including Adobe Acrobat, ColdFusion and ColdFusion Builder.

A problémát nem az adatok hiánya jelenti

"Target appears to have failed to respond to **multiple warnings from the company's anti-intrusion software** …"

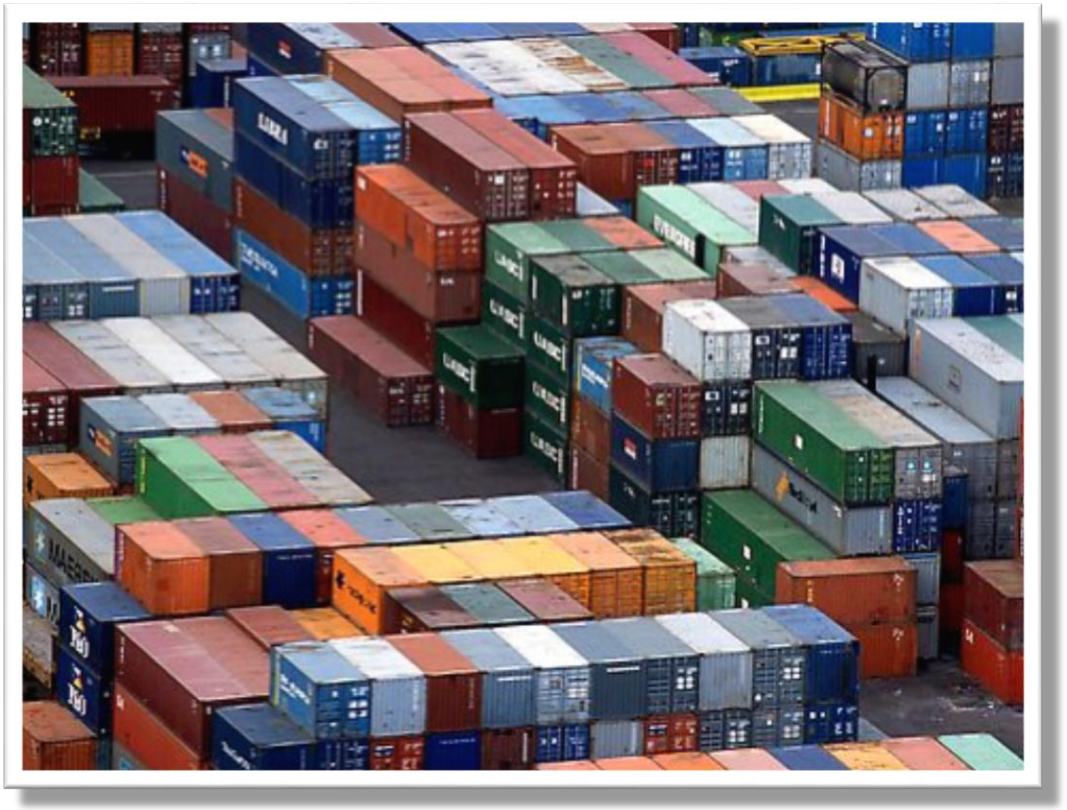
- A "Kill Chain" Analysis of the 2013 Target Data Breach, March 26, 2014

"Neiman Marcus Hackers Set Off **60,000 Alerts** While Bagging Credit Card Data."

– Ben Elgin, Dune lawrence, Michael Riley, February 21, 2014

Túl sok zaj, **nem elég hasznos információ**

Azonosítani kell a **szokatlan tevékenységeket**



SIEM megoldások kiegészítése

Jogosultságok, személyazonosság információk

Konfiguráció kezelés

Tevékenység figyelés

SIEM megoldások kiegészítése

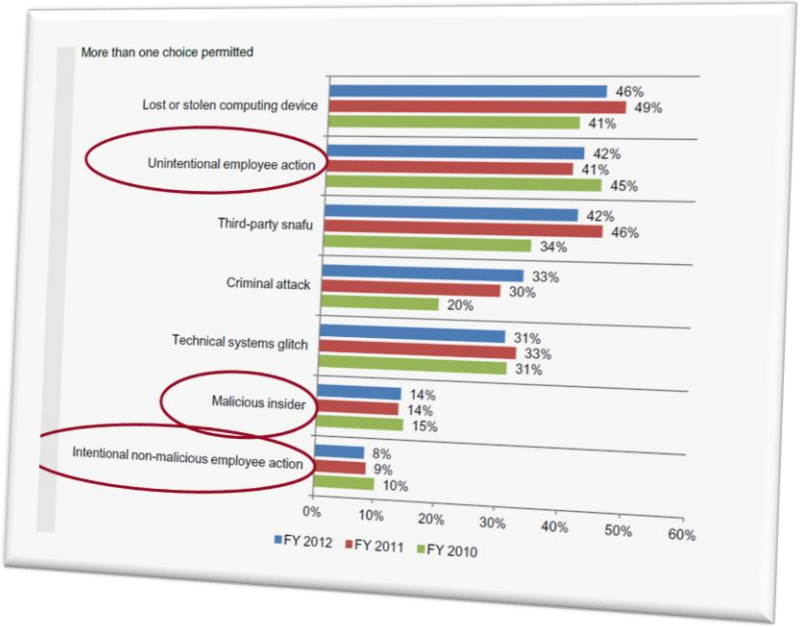
Jogosultságok, személyazonosság információk

Konfiguráció kezelés

Tevékenység figyelés

A felhasználó a leggyengébb láncszem

- Adathalászat
- Fájlmegosztók
- Hordozható eszközök
- Konfigurációs hibák
- Alkalmazottak
  - Elégedetlenek
  - Naívak
  - Szabotőrök
  - Felbéreltek



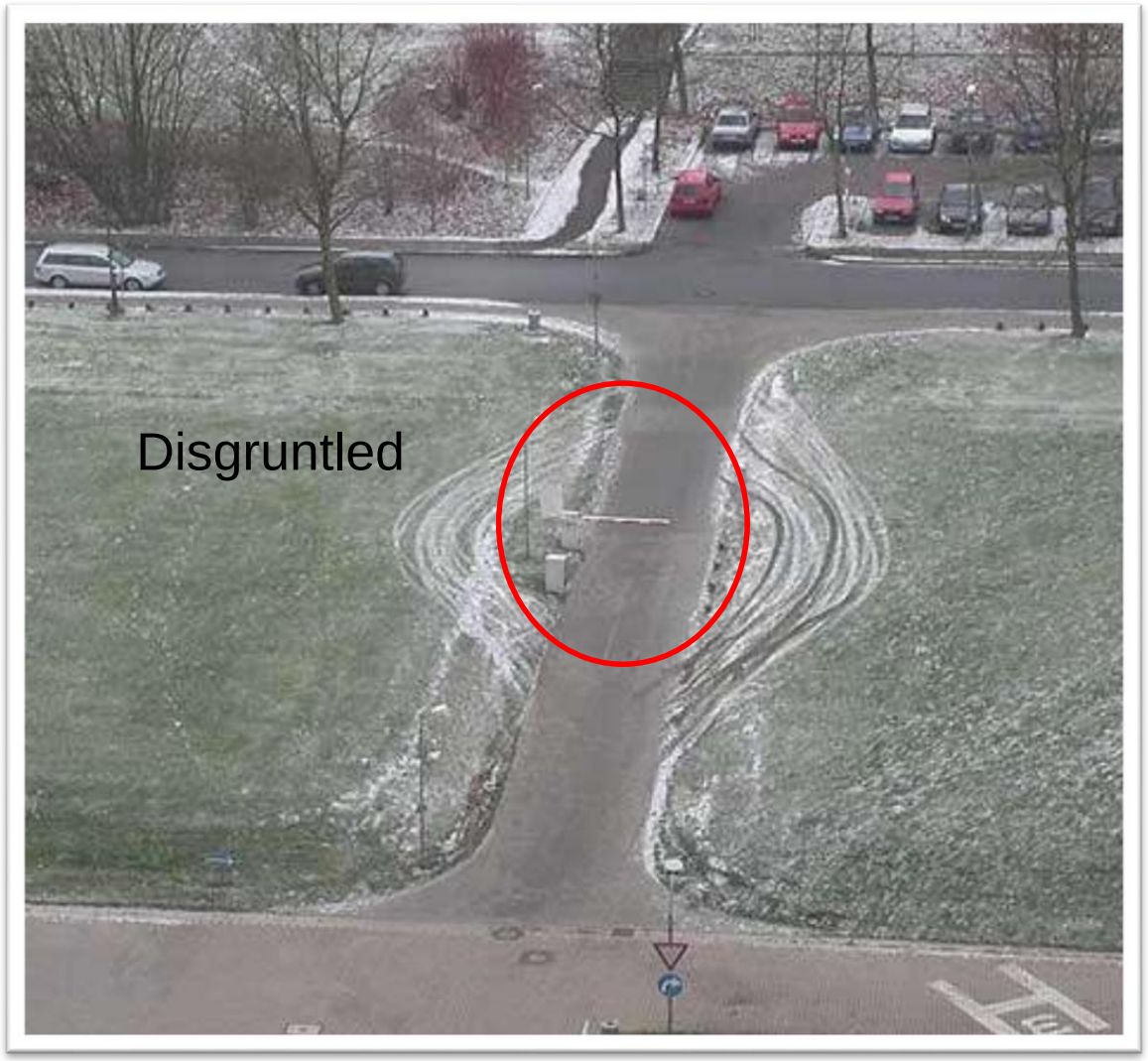
Source: Third Annual Benchmark Study on Patient Privacy & Data Security – Ponemon Research

Személyazonosság információk felhasználása

- A felesleges jogosultságok megszűntetése, csökkentése
- Rendszergazdai jogosultságok menedzselése, figyelése
- SIEM eszközök integrációja IDM rendszerekkel
- SIEM rendszerek integrációja hálózati eszközökkel

A korlátozás nem elég

Megfigyelés is szükséges



SIEM megoldások kiegészítése

Jogosultságok, személyazonosság információk

Konfiguráció kezelés

Tevékenység figyelés

Tevékenységfigyelés
A legfontosabb kérdések

Milyen változások történtek?

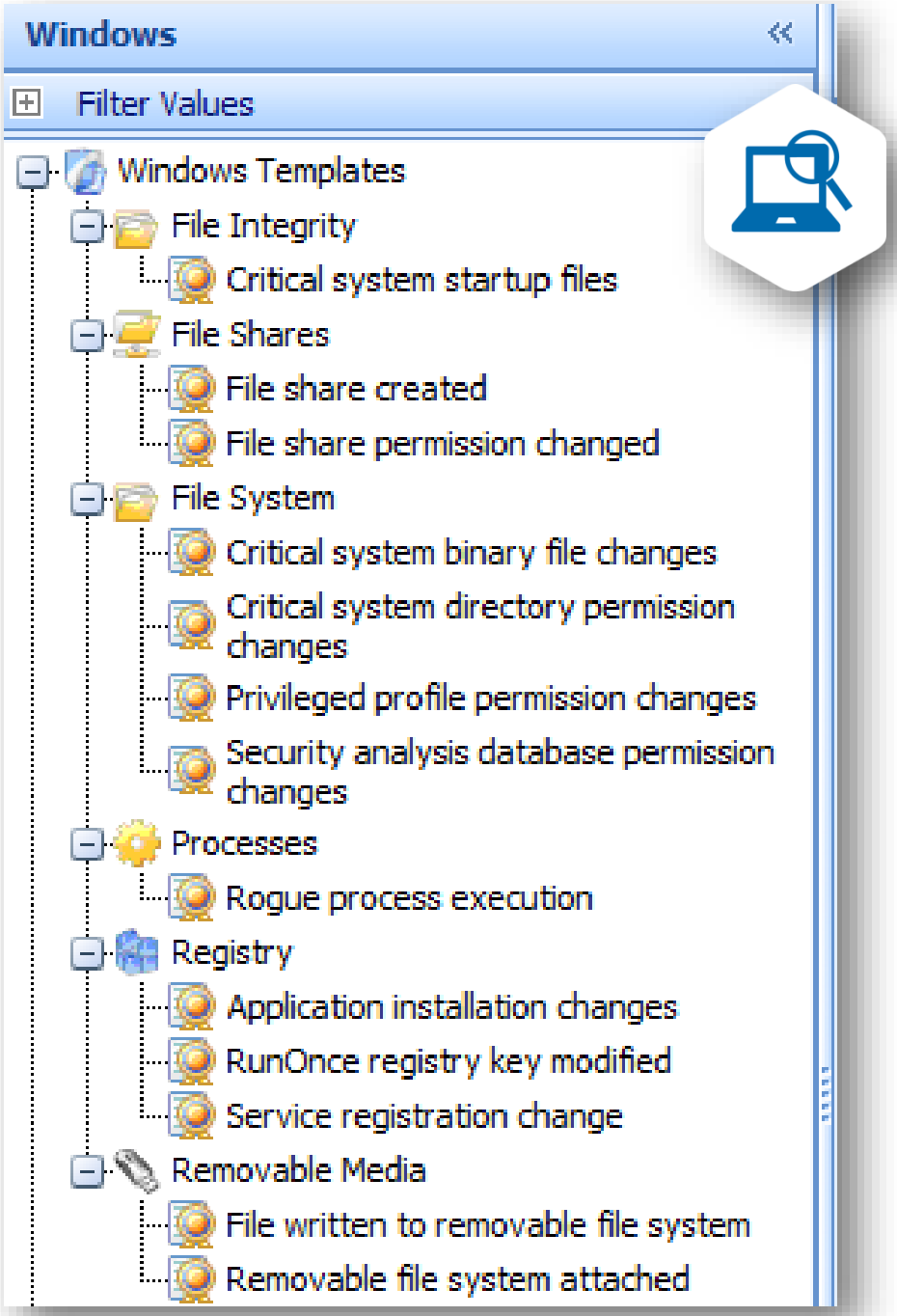
Mikor történtek a változtatások?

Ki követte el ezeket?

Honnan végezték el a változtatásokat?

Jóváhagyott változtatások voltak?

Mit figyeljünk?



SIEM megoldások kiegészítése

Jogosultságok, személyazonosság információk

Konfiguráció kezelés

Tevékenység figyelés

Konfigurációkezelés

- Konfigurációk és felhasználói jogosultságok felmérése
- Ajánlott konfigurációk (CIS, NIST, SANS)
- Biztonsági rések felderítése
- Peremfeltételek meghatározása és változásjelentések készítése

SIEM megoldások kiegészítése

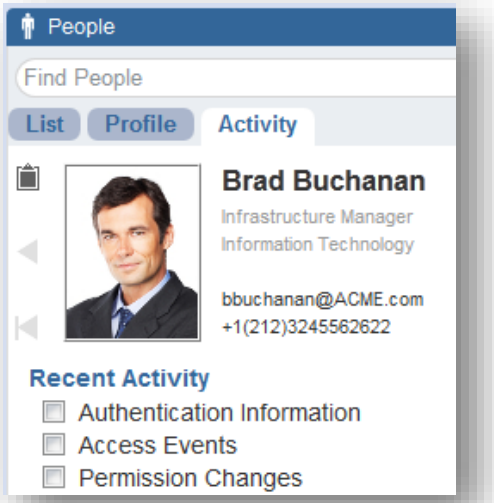
Jogosultságok, személyazonosság információk

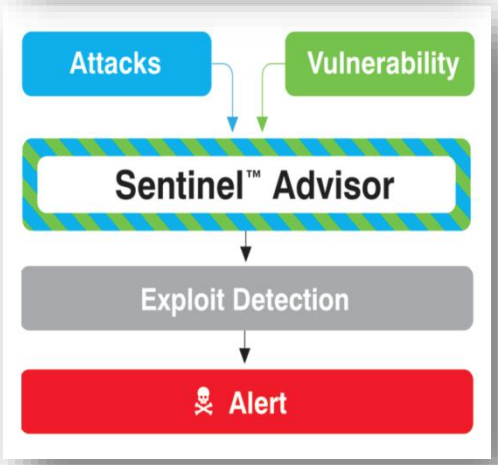
Konfiguráció kezelés

Változás figyelés

Egy példa

- **IDM integráció:** Személyazonosság alapú tevékenység figyelés
- **Mobil és hálózati eszköz integráció:** Felhasználók/eszközök
- **Fenyegetés + Sérülékenység:** Támadás, vagy próbálkozás
- **Tevékenységfigyelés:** Konfiguráció változások észlelése





Worldwide Headquarters
515 Post Oak Blvd.,
Suite 1200
Houston, TX 77027 USA

+1 713.548.1700 (Worldwide)
888.323.6768 (Toll-free)
info@netiq.com
NetIQ.com

www.netiq.com/communities

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.