# SIEM (Security Information and Event Management)

**SIEM** je softwarové řešení, které kombinuje dvě dříve oddělené oblasti:

- **SIM (Security Information Management):** Sběr, ukládání a analýza logů pro účely reportingu a souladu s předpisy (compliance).
- **SEM (Security Event Management):** Monitorování událostí v reálném čase, korelace dat a upozorňování na incidenty.

Hlavním úkolem SIEMu je poskytnout bezpečnostním analytikům ucelený přehled o tom, co se děje v celé IT infrastruktuře (od serverů přes firewally až po koncové stanice).

## Jak SIEM funguje? (Životní cyklus dat)

Proces fungování SIEMu lze rozdělit do několika fází:

1. **Sběr dat (Data Aggregation):** Agreguje logy z různých zdrojů – síťová zařízení, servery, databáze, antiviry a cloudové služby.
2. **Normalizace:** Převádí nesourodá data z různých zařízení do jednotného formátu (např. aby „User Login“ z Windows a „Access Granted“ z Linuxu vypadaly pro systém stejně).
3. **Korelace:** Nejdůležitější část. SIEM hledá vztahy mezi událostmi.
    - *Příklad:* 5 neúspěšných přihlášení na server následovaných jedním úspěšným z IP adresy v jiné zemi spustí poplach (možný Brute Force útok).
4. **Upozorňování (Alerting):** Pokud systém detekuje shodu s pravidlem nebo anomálii, okamžitě informuje bezpečnostní tým (SOC).

## Proč je SIEM nezbytný?

Bez SIEMu by museli analytici kontrolovat logy každého zařízení zvlášť, což je v moderních sítích nemožné. SIEM řeší:

- **Detekce pokročilých hrozeb (APT):** Odhalí útočníka, který se v síti pohybuje nenápadně.
- **Compliance (Audit):** Pomáhá splnit zákonné požadavky na uchovávání a ochranu dat (např. GDPR, NIS2, ISO 27001).
- **Zkrácení doby odezvy:** Dramaticky zrychluje reakci na incident (snižuje tzv. **MTTR** - Mean Time To Respond).

## Srovnání: SIEM vs. Log Management

| Vlastnost | Log Management (např. standardní ELK Stack) | SIEM |
|---|---|---|
| **Primární účel** | Sběr a vyhledávání v logách. | Bezpečnost a reakce na hrozby. |
| **Korelace** | Obvykle chybí nebo je omezená. | Pokročilá korelace napříč zdroji. |

| Vlastnost | Log Management (např. standardní ELK Stack) | SIEM |
|---|---|---|
| **Pravidla** | Zaměřena na provozní chyby. | Zaměřena na hackerské techniky. |
| **Hlášení** | Výkonnostní grafy. | Bezpečnostní incidenty a audity. |

# Moderní trendy: SIEM + SOAR + UEBA

Dnešní SIEM systémy jsou často rozšiřovány o:

- **UEBA (User and Entity Behavior Analytics):** Využívá strojové učení k detekci „divného“ chování uživatelů (např. když účet účetní začne v noci stahovat data z databáze programátorů).
- **SOAR (Security Orchestration, Automation and Response):** Umožňuje na útok reagovat automaticky (např. při detekci viru automaticky odpojit infikovaný počítač od sítě).

> **Příklady SIEM nástrojů:** Splunk, IBM QRadar, Microsoft Sentinel, LogRhythm nebo open-source varianty jako **Wazuh** (často postavený nad ELK Stackem).

— **Viz také:** ELK Stack, Cloud Monitoring, IDS/IPS, SOC (Security Operations Center)