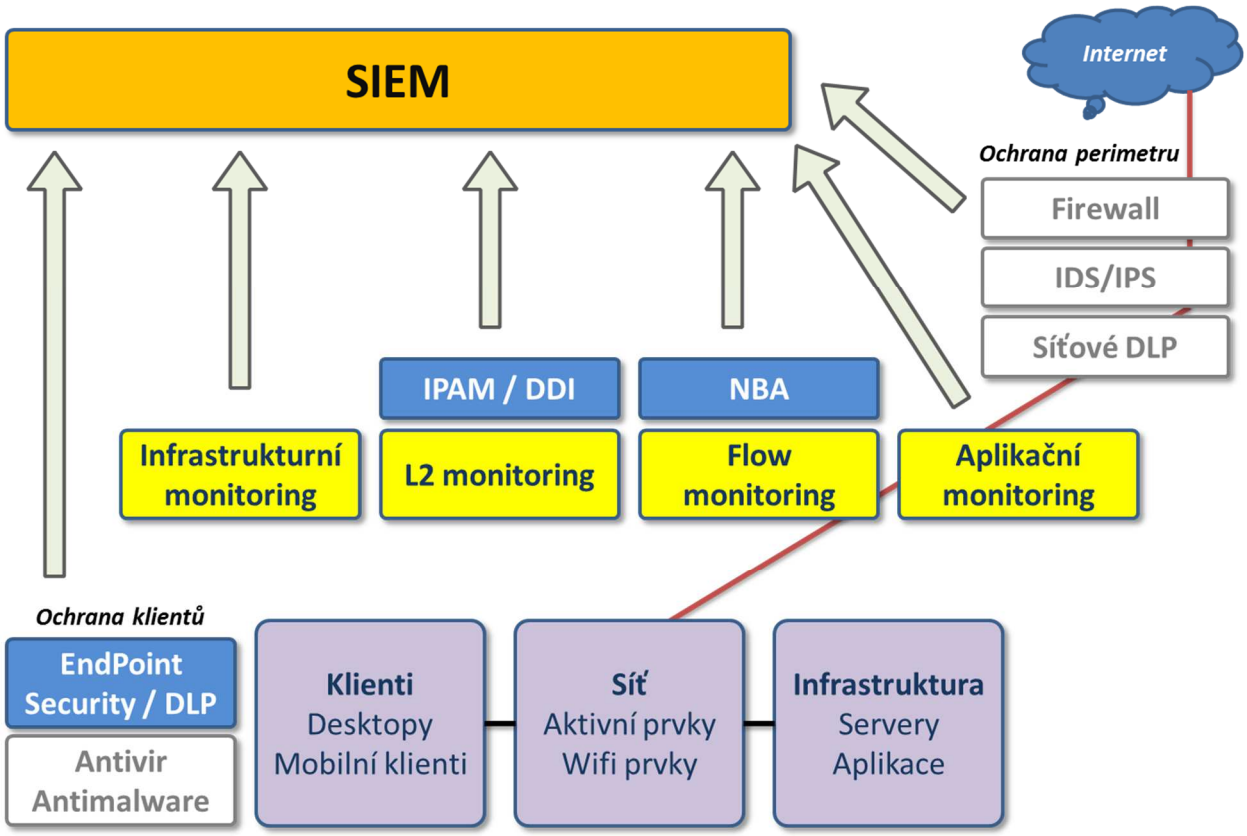
# Koncept aktivní bezpečnosti sítě

*Koncept aktivní bezpečnosti, připravený ve spolupráci předních českých výrobců a bezpečnostních odborníků, je připravený na nové požadavky a výzvy, které v oblasti informační bezpečnosti přináší propojený svět komunikací. Reaguje rovněž na nové požadavky, které na tuto oblast klade platná i připravovaná Česká a Evropská legislativa.*




Koncept respektuje běžné fungování a zvyklosti organizací v oblasti informačních technologií a při práci s daty. Do běžné infrastruktury organizace přidává sofistikované monitorovací nástroje a metody. Ty jsou dále nadstandardním způsobem doplněné o integrované nástroje pokročilé analýzy datových toků (NBA – Network Behaviour Analysis) s nástroji pro komplexní správu IP adresního prostoru a řízením přístupů pevných i mobilních zařízení do sítě (IPAM/DDI/NAC). Tyto nástroje mohou být vhodně doplněny nástrojem komplexní ochrany klienta (End Point Security).

Samozřejmostí je koexistence s běžnými komponentami ochrany perimetru (Firewall, IDS/IPS, DLP apod.) a klientů (Antivir, Antimallware, Antispam apod.).

Dílčí komponenty konceptu poskytují informace, které jsou na operativní úrovni vyhodnocované jako signifikantní (překročující například nastavené prahové úrovně), nadstavbovému nástroji SIEM (Security Information and Event Management). Tento nástroj sbíraná data koreluje a inteligentně vyhodnocuje závažnost jednotlivých incidentů. Obsluze pak přehledným způsobem prezentuje informace o zaznamenaných hrozbách a předkládá návrhy na potřebné reakce.

Díky tomu, že v rámci konceptu jsou obsaženy i nástroje aktivně řídící síťovou infrastrukturu, a to včetně řízení přístupů na síť, může obsluha SIEM systému například okamžitě vypnout síťovou komunikaci kompromitovaného zařízení a eliminovat tím riziko spojené s jeho další možnou komunikací na síti.

Velkou výhodou konceptu a nadstavbového SIEM systému je, že plně odpovídá zvyklostem a požadavkům v oblasti bezpečnosti informačních technologií a to jak z hlediska funkčního, tak i procesního – kdy plně podporuje požadavky kladené v rámci ISO27000.

Vedle nesporných funkčních přínosů celého konceptu je další výhodou rovněž know-how a ověřené projektové postupy, které jsou zákazníkům k dispozici jak při návrhu a implementaci, tak i při následné podpoře.

Koncept je možné zavádět najednou komplexně nebo postupně podle priorit zákazníka zavádět jeho dílčí komponenty. V případě postupné implementace je garantována vzájemná provázanost a interoperabilita klíčových komponent konceptu.

***Na rozdíl od dílčích komponent bezpečnosti a samostatných bezpečnostních nadstaveb přináší tento koncept navíc unikátní integrované nástroje pro okamžitou realizaci aktivní zásahů.***

**Koncept se opírá o následující klíčové a integrované komponenty:**

**Monitoring**

- **MoNet** – monitoring infrastruktury a aplikací
- **AddNet** – L2 monitoring sítě
- **FlowMon** – monitoring datového provozu
- **FerretApps** – pokročilý monitoring aplikací

**Behaviorální analýza sítě**

- **FlowMon ADS**

**Řízení přístupu do sítě**

- **AddNet/ AddNet BYOD**

**SIEM**

- **Trustwave SIEM / Balabit SIEM**

**Doplňkově - EndPoint security**

- **Safetica**

***Tento koncept je v úzké kooperaci prezentován skupinou předních českých výrobců a specialistů na informační bezpečnost.***

**Novicom INVEA-TECH FerretApps Axenta**