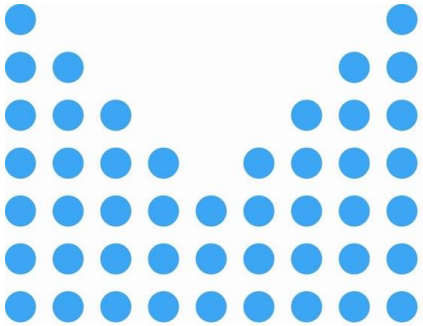
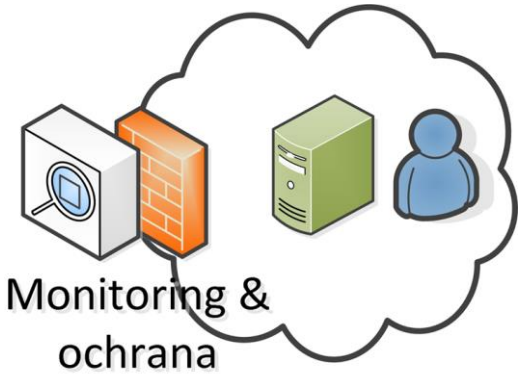


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Sdílení a analýza bezpečnostních událostí v ČR

Motivace

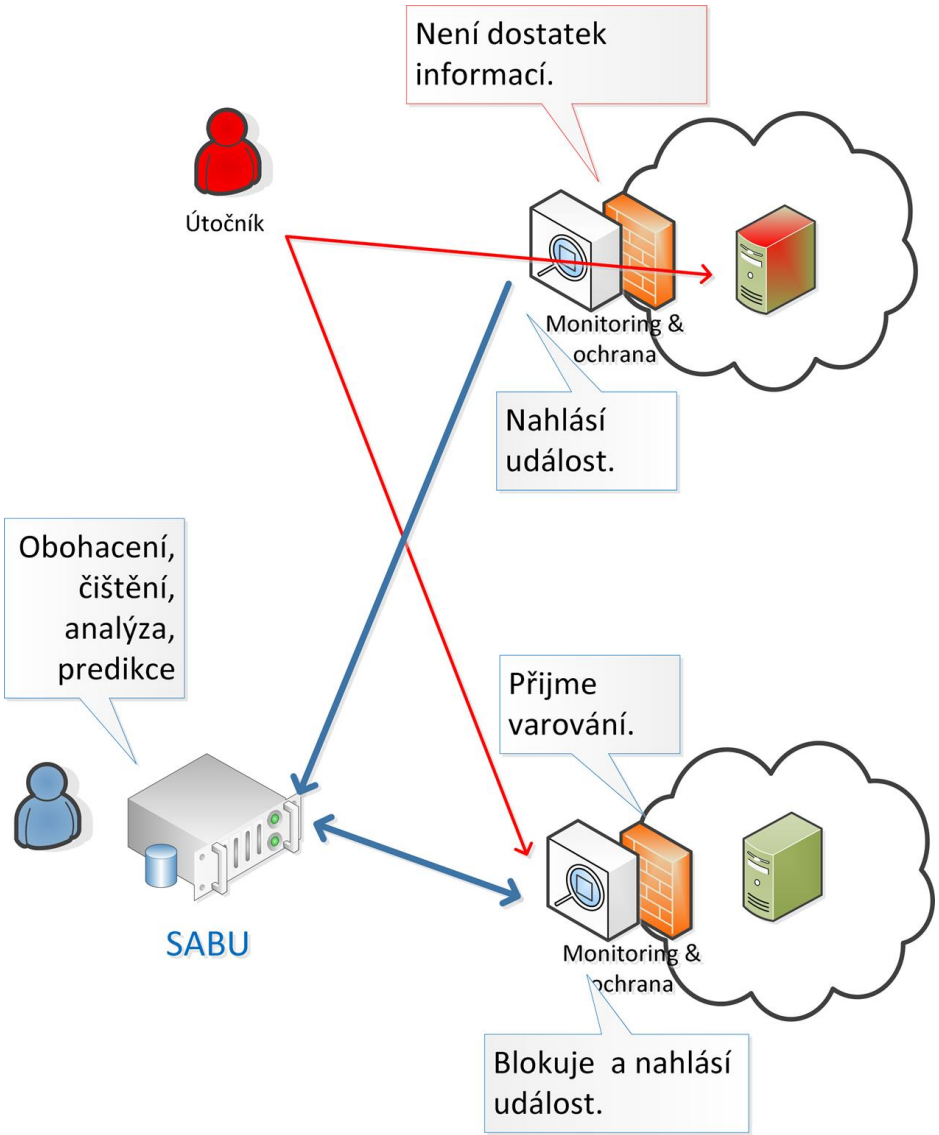
Sítě jsou přirozeně nezávislé a řeší bezpečnost odděleně



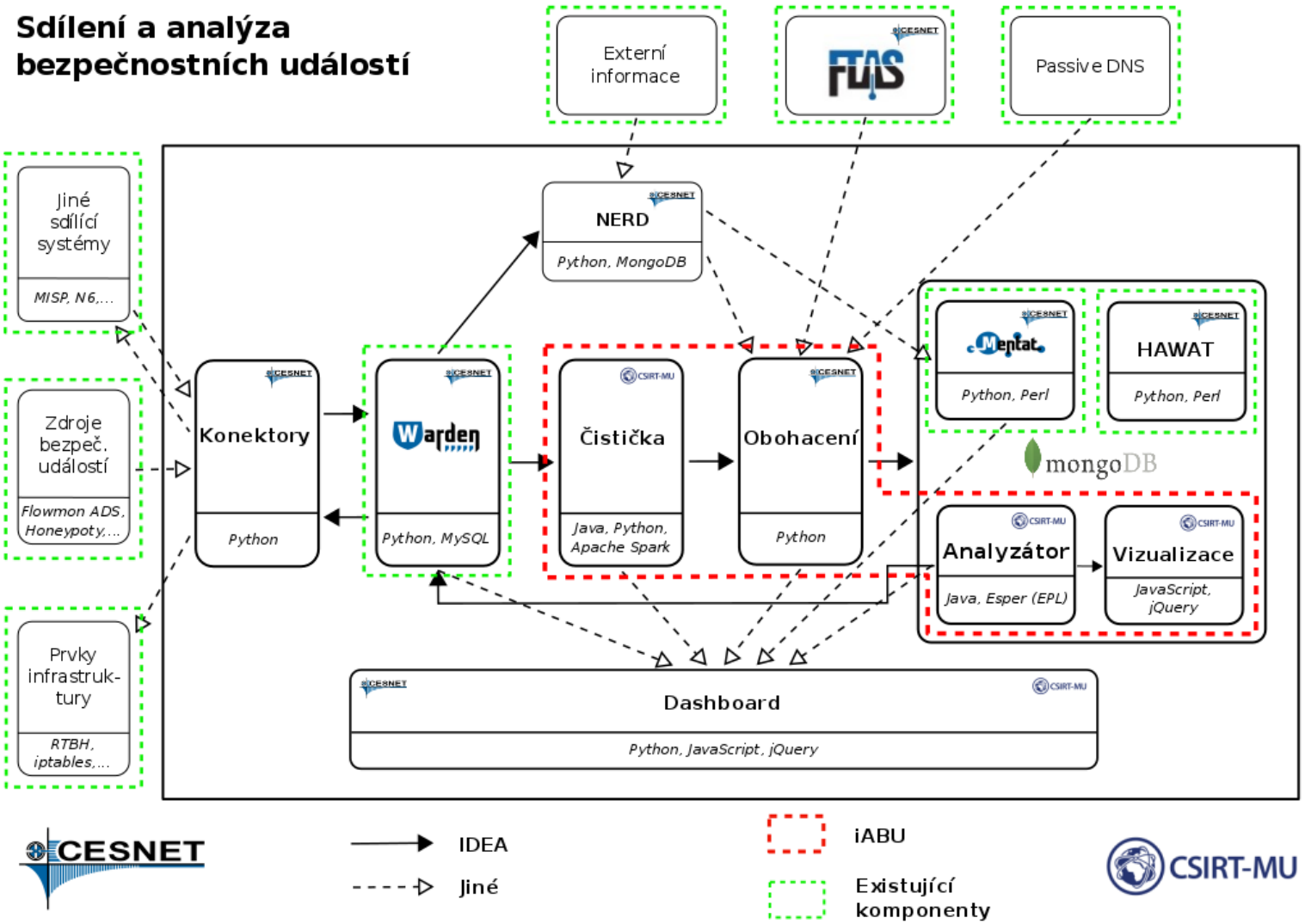
Neexistuje předávání informací a jejich využití

Motivace

- Sdílení, obohacení a korelace dovolí **efektivnější reakci**



Architektura



Konektory

- Vstupní - jednoduché napojení Vašeho detekčního systému na Warden
  - Transformace reportu na IDEA zprávu
  - Validace
  - Filtrace
  - Anonymizace
- Výstupní – jednoduché napojení výsledků analýzy na prvek ochrany infrastruktury
  - Definice politik

iABU

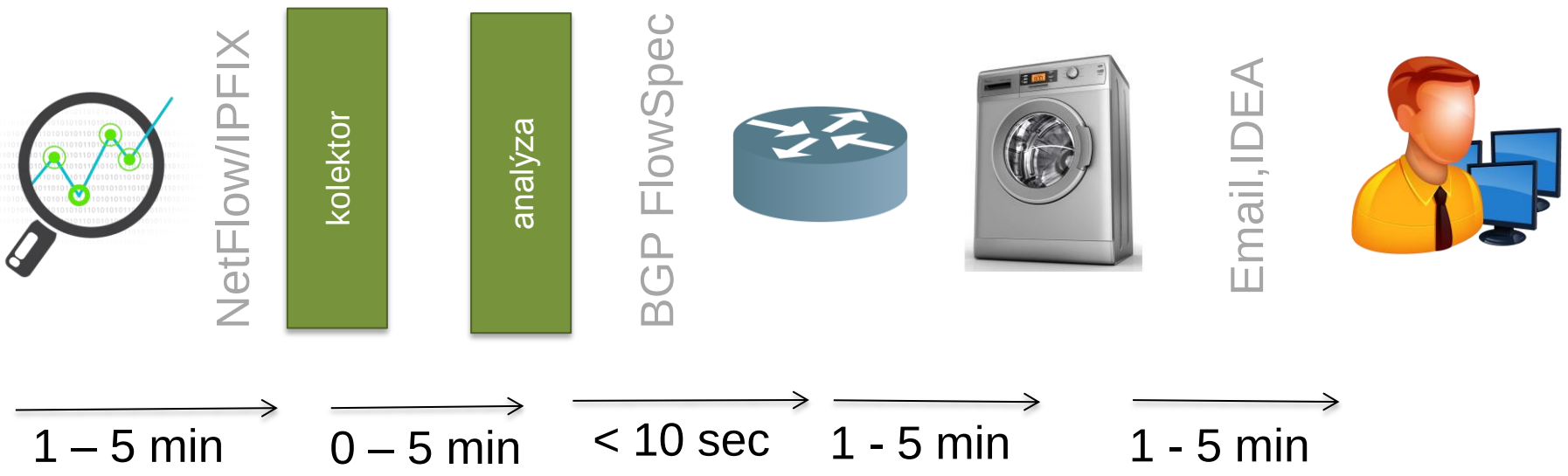
- Inteligentní analýza bezpečnostních událostí
  - Čištění událostí
  - Analýza
  - Vizualizace
  - Dashboard

Obohacení

- Vstupní data jsou obohacena o data třetích stran ale i o data vlastní
- Blacklisty, geolokace, shodan.io, …
- Flow data, logy, …
- Technologie pro zpracování IntelMQ
- NERD

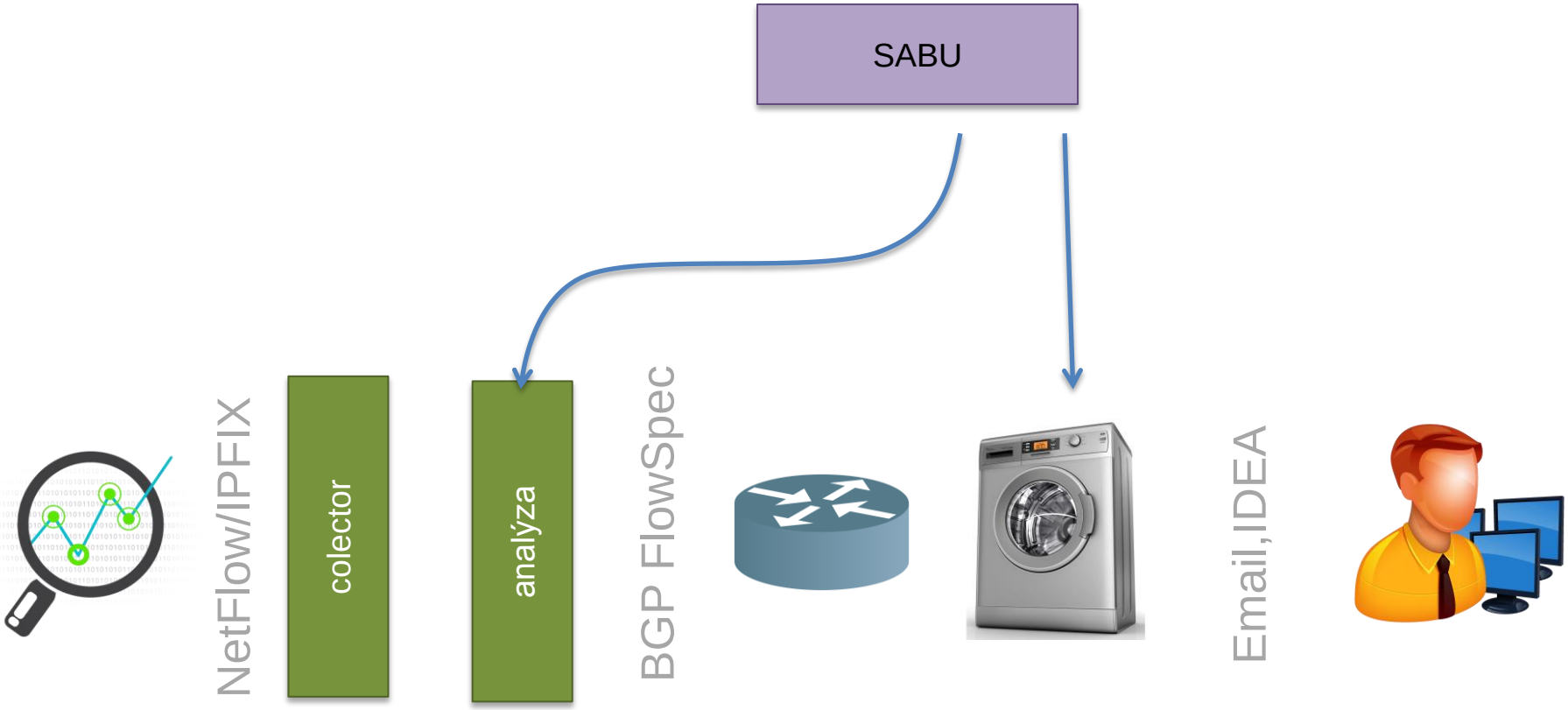
Příklad použití

- Dlouhá doba reakce na DDoS



Příklad použití

- Zrychlení reakce použitím SABU - NERD



Shrnutí

- Jednoduché připojení do sdílení
- Souhrn dat z vnitřních a externích zdrojů
- Analýza dat → reputační DB, trendy a vizualizace
- Jednoduchá a parametrizovatelná mitigace