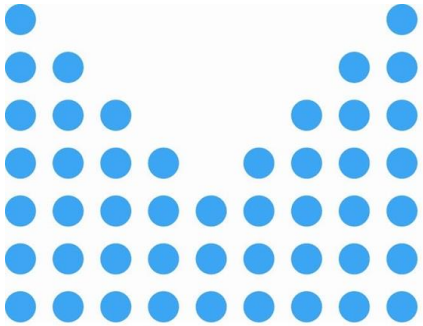


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Sdílení a analýza bezpečnostních událostí v ČR

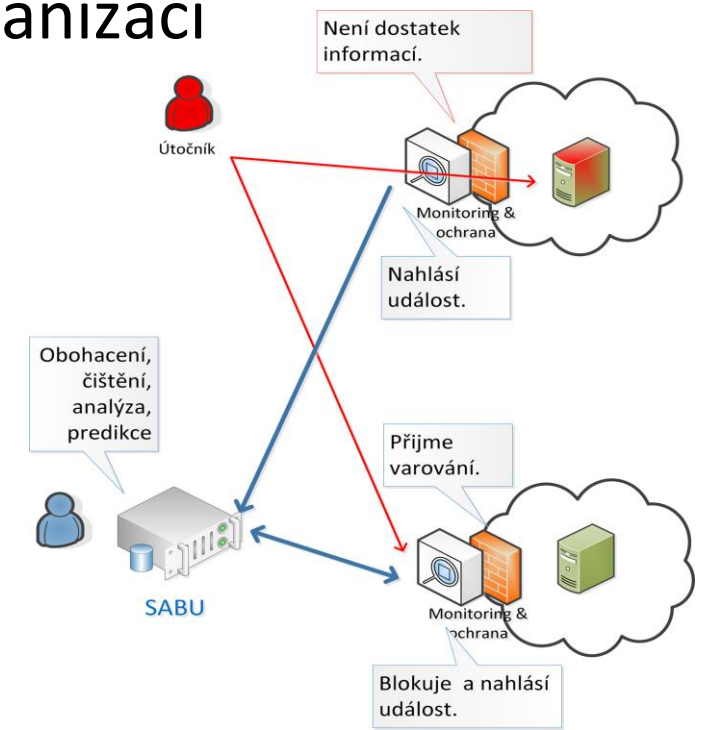
Přivítání

- Organizační informace
- Program semináře

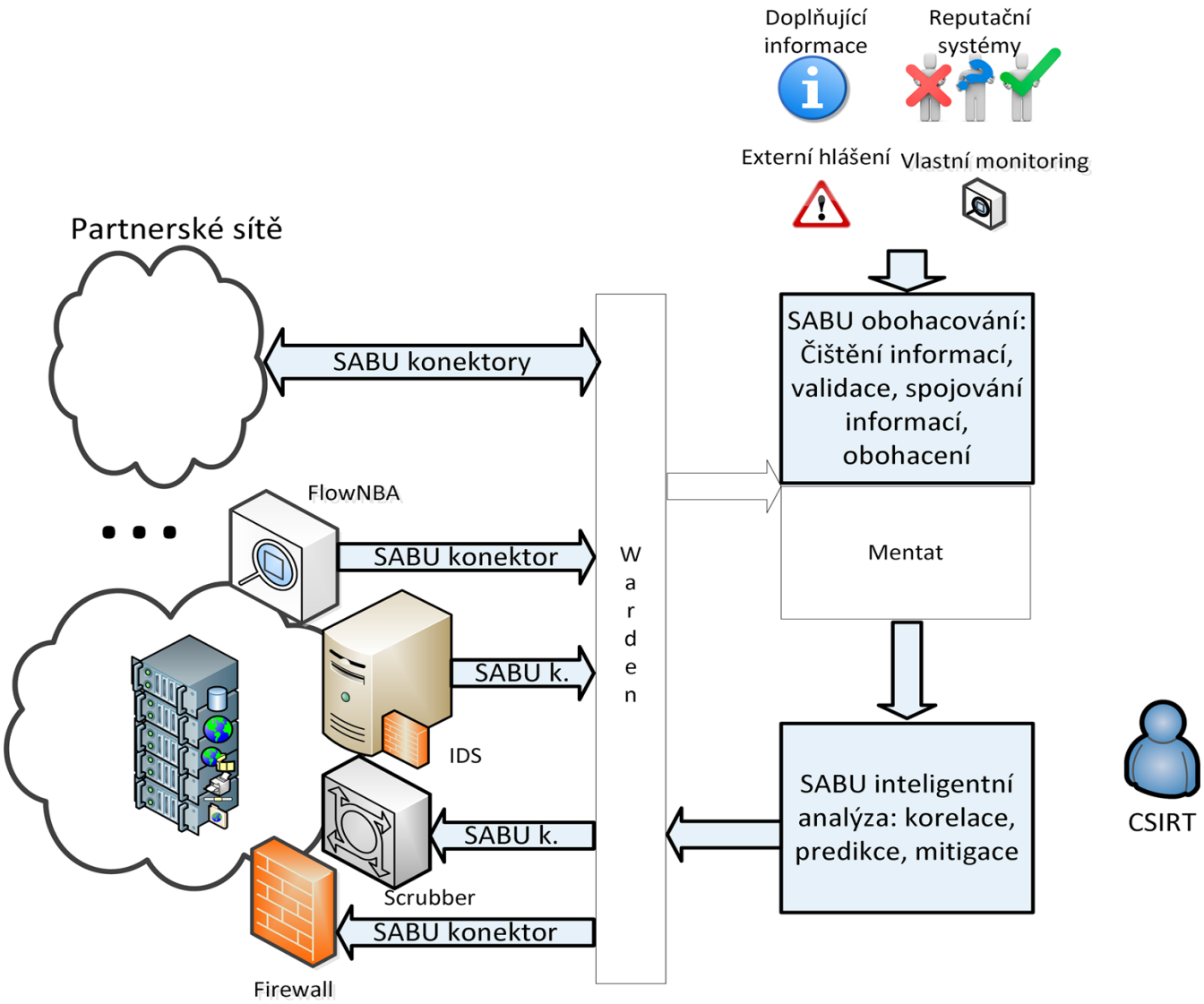
8:45 Dema
9:15 SABU stav
9:25 Architektura SABU
9:45 Deduplikace zpráv
10:15 Reputace
10:45 Passive DNS
11:15 Měření výkonnosti DB pro SABU
11:45 Právní aspekty
14:00 Tutoriál: Jak se připojit k Warden
14:30 Diskuse
15:00 PROKI

Cíle

- Hlavním cílem projektu je vytvoření pilotního systému pro sdílení a analýzu bezpečnostních událostí v ČR
  - Rozšířit sdílení do dalších organizací
  - Obohacování událostí
  - Pokročilou analýza dat
  - Zvýšit bezpečnost sítí skrze mitigaci



Schéma


Doplňující informace
Reputační systémy
Externí hlášení
Vlastní monitoring
Partnerské sítě
SABU konektory
SABU obohacování: Čištění informací, validace, spojování informací, obohacení
FlowNBA
SABU konektor
Mentat
SABU k.
IDS
W a r d e n
SABU inteligentní analýza: korelace, predikce, mitigace
CSIRT
SABU k.
Scrubber
SABU konektor
Firewall

Stav

- Rešerše stávajícího stavu
- Specifikace konektorů
- Specifikace inteligentní analýzy
- Specifikace obohacování dat
- Implementace konektorů
  - Flowmon
  - honeypoty
  - Beekeeper
  - IntelMQ

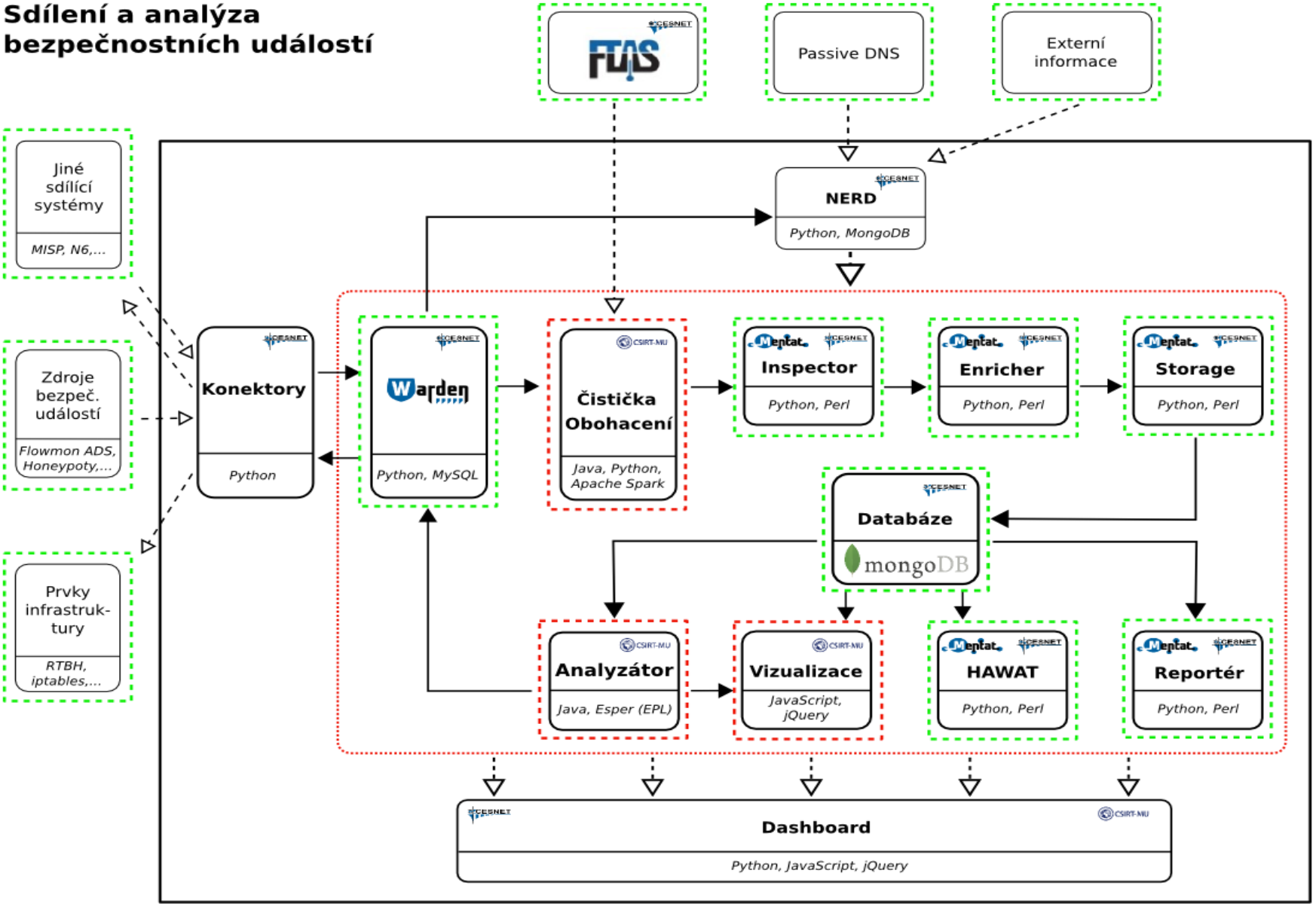
Stav

- PR skrze akce (ISACA a další)
- Připojování nových členů (CSIRT.SK, …)
- Publikace (deduplikace, time-machine)
- Setkání s partnery

Architektura

- Návrh architektury systému SABU
  - značně heterogenní systém
  - každá část má svá specifika

Sdílení a analýza bezpečnostních událostí



CESNET

IDEA

Jiné

iABU

Existující komponenty

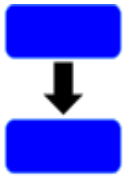
CSIRT-MU

Konektory

- Vytipování vhodných zdrojů událostí
  - Vstup: FlowmonADS, Kippo, Dionea, Beekeeper, IntelMQ, HP Tipping Point
  - Výstup: textový report
- Definice činností vstup. konektoru
  - Příjem
  - Konverze
  - Filtrování
  - Anonymizace
  - Information Exchange Policy

Konektory



Input
- Socket
- File
- Files
- SysLog
- HTTP
- Warden
- DB
- XMPP
- HPFeeds

Parse
- Mail
- CSV
- JSON
- Regex

Cast
- Normalize
- Anonymize

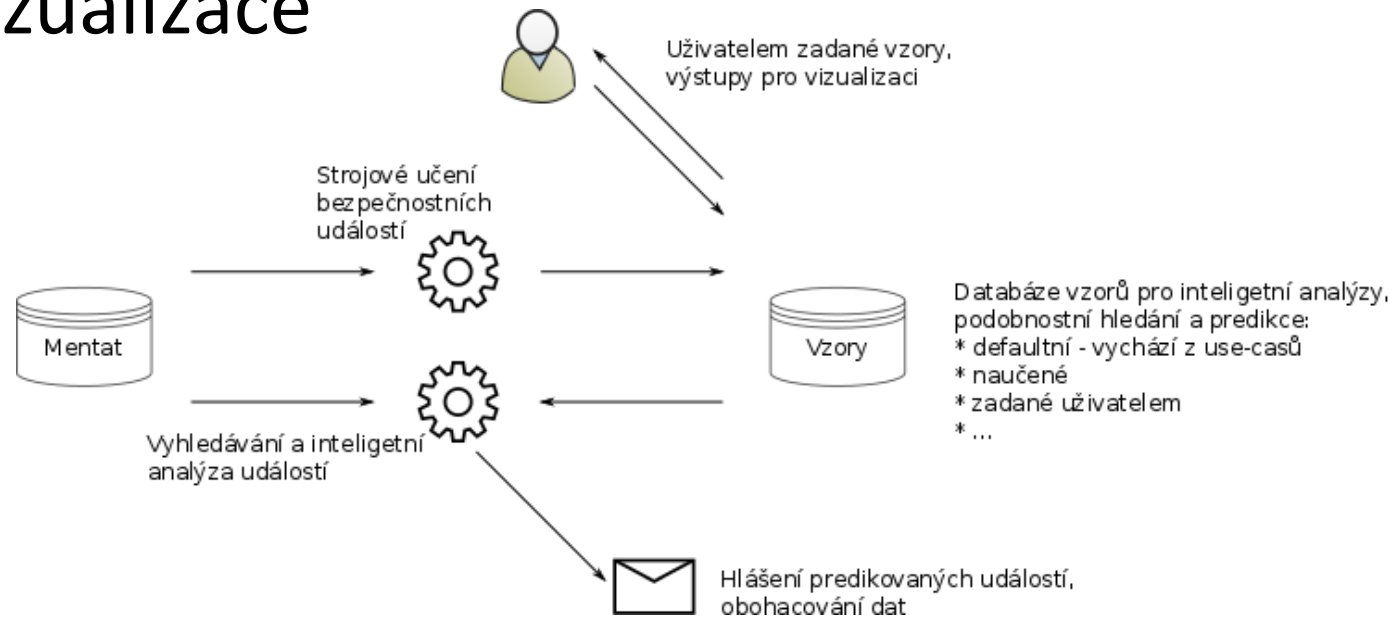
Convert
- Static
- Generator
- Exec

Process
- Deduplicator
- Aggregator
- RateLimiter
- Filter

Output
- Socket
- File
- Files
- SysLog
- Warden
- DB
- XMPP
- HPFeeds

iABU

- Agregace
  - Duplikáty, pokračující, překrývající
- Analýza
  - Učení vzorů, ukládání, vyhledávání, rozhodování
- Vizualizace



Obohacení

- Události z Warden jsou obohaceny o data třetích stran
- Data jsou asociována k entitě (IP adrese, prefixu, hostname)
- Blacklisty, geolokace, shodan.io, …
- Při příchodu události se provede dotaz do NERD

Shrnutí

- Jednoduché připojení do sdílení
- Souhrn dat z vnitřních a externích zdrojů
- Analýza dat pro vyhledávání vzorů a predikci útoků
- Uplatnění výstupů analýzy při značení podezřelého provozu a k mitigaci útoků