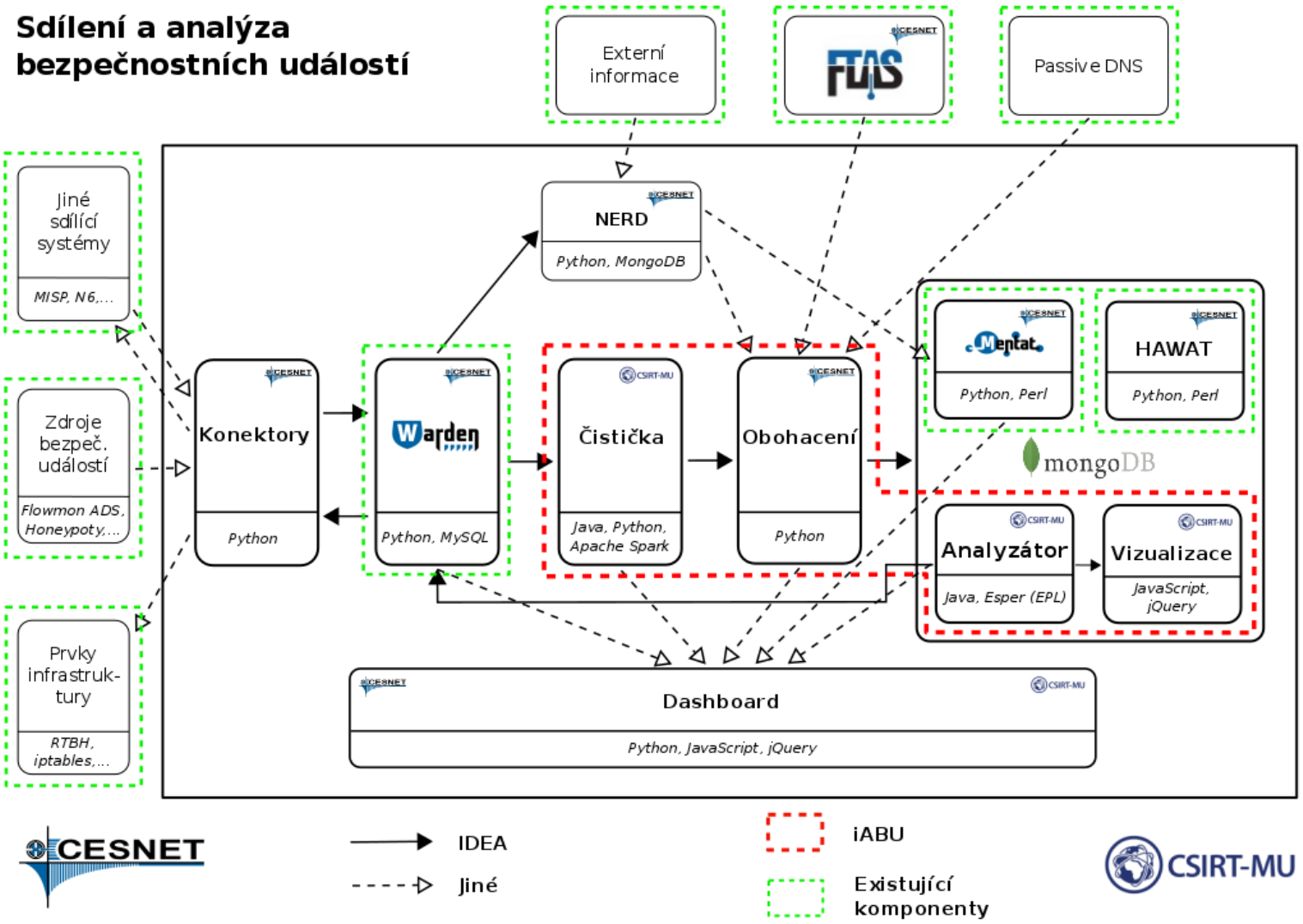
Inteligentní analýza bezpečnostních událostí (iABU)

Jan Vykopal

20. 6. 2016

Architektura



iABU

- Inteligentní analýza bezpečnostních událostí
  - Čištění událostí
  - Analýza
  - Vizualizace
  - Dashboard
  - Obohacení
    - NERD – jeden ze zdrojů, více v další prezentaci

Čistička událostí

- Umístěna mezi zdrojem dat (Wardenem) a úložištěm (Mentatem)
- Filtruje (deduplikuje) a upravuje (doplňuje) přicházející události
- Klíčová pro další komponenty, které už budou pracovat s tím, že každá událost je **validní** a uložena a **analyzována právě jednou**
- Odstraňuje chybné události, které by mohly negativně ovlivnit výsledky návazných analýz

Čistička – případy použití I

- Jemné síto na data z Wardenu
  - Základní filtrace nevalidních událostí na vstupu
  - Příklady:
    - špatný formát dat (nesmyslný port, nevalidní adresa)
    - klient nahlásí událost z adresního rozsahu, který mu nepřísluší
    - neodpovídající čas detekce (příliš v minulosti nebo v budoucnosti)
    - IP adresy nebo domény známých služeb (Google, Wikipedia, Facebook, ….)
    - IP adresy týkající se lokální sítě (127.0.0.1, broadcast IP, ...)
    - jako zdroj útoku je označen NAT, proxy nebo jakákoliv jiná relay

Čistička – případy použití II

- Agregace dvou a více událostí stejného typu pocházejících ze stejného zdroje
  - Jeden z více modulů čističky
  - Příklad:
    1. Detekce události horizontálního skenování portu 22 z IP adresy *A* v čase *t*
    2. Detekce další události stejného typu v čase *t+300 s*
    3. Detekce další události (poslední) v čase *t+600 s*

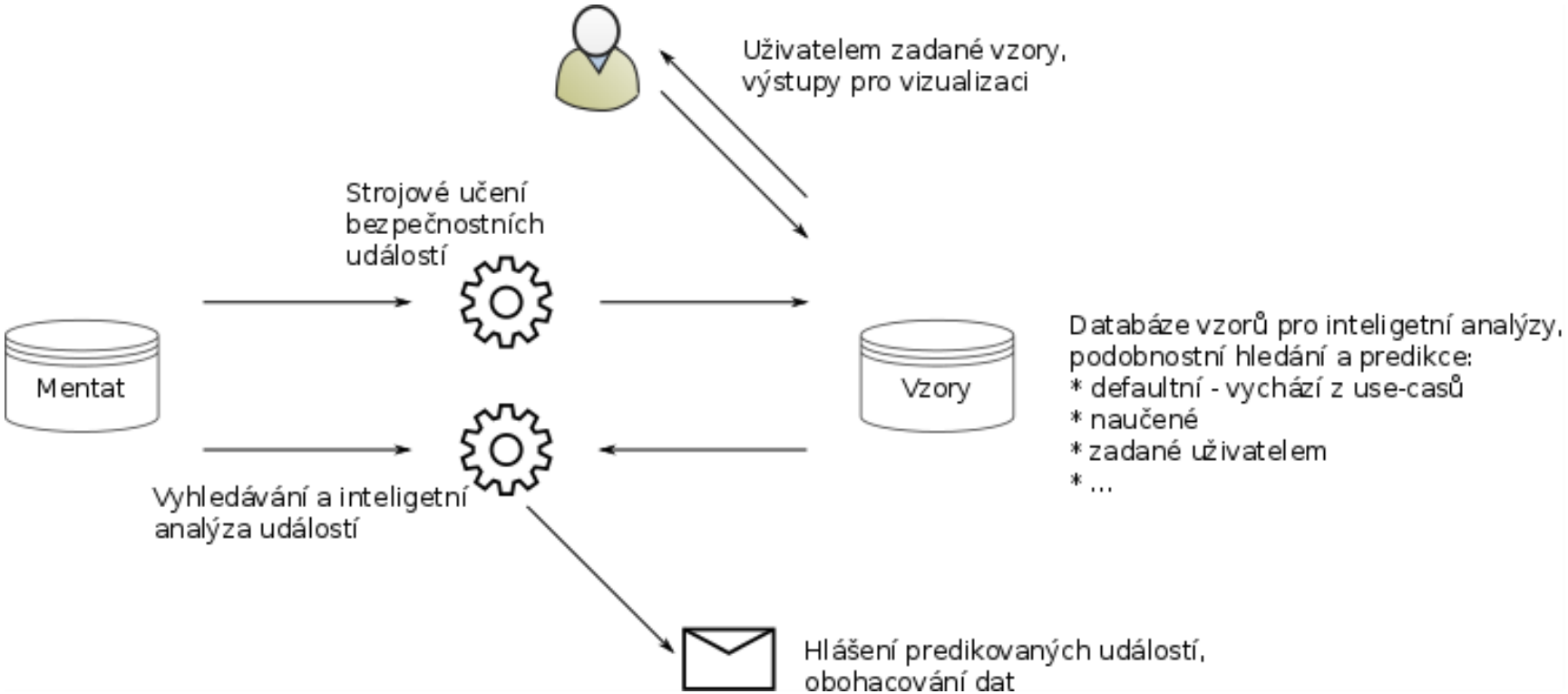
Obohacení událostí

- Události nesou v sobě identifikátory (typicky IP adresy), ke kterým mohou existovat dodatečné informace
- Pro komplexnější analýzu je výhodné přidat tyto informace k dané události (= obohatit ji)
- Příklady obohacení:
  - Geolokační a administrativní informace
  - Role stroje v síti
  - NERD – Network Entity Reputation Database

Analyzátor událostí

- Součást Mentatu, která má přístup k datovému úložišti
- Spoléhá se na kvalitní data, která prošla čističkou
- Klíčová komponenta pro pokročilé analýzy událostí
  - Souvislost mezi událostmi (korelace)
  - Vyhledávání komplexních událostí
  - Predikce útoků a hrozeb

Analyzátor – učení vzorů



Příklady vzorů I

Souslednost událostí

- Skupina vzorů, ne pouze jeden
- Příklad:

1. Agregovaná a ukončená událost skenování SIP portu na IP adrese *B* z IP adresy *A* v čase *t*
2. Agregovaná a ukončená událost hádání hesla z IP adresy *C* na *B* v čase *t + 1000 s*
3. Agregovaná událost o podezřelých voláních z IP adresy *B* v čase *t + 1010 s*

Příklady vzorů II

Souvislost mezi událostmi různého typu

- Příklad:

1. Směrovače organizace *X* zahodí velké množství paketů na základě reverse path filtering (RPF) v čase *t* a nahlásí tuto událost
2. Organizace *Y* detekuje amplifikační DoS na svou infrastrukturu v čase *t - 10 s*

Predikce útoků a hrozeb

- Na základě částečné shody se vzorem
- Může mít návaznost na mitigační konektory, události tohoto typu musí být jasně označeny
- Příklady:
  - skenování portů – slovníkový útok – nahrání malware
  - útočník již skenoval čtyři české sítě => pravděpodobně bude skenovat i ostatní české sítě
  - útočník v jedné síti skenoval a pak spustil slovníkový útok + vidíme, že v jiné síti skenuje => čekáme slovníkový útok

Určování závažnosti

- Na základě korelace události s ostatními událostmi a výstupy analýzy a obohacení.
- Závažnost je dána **typem** a **rozsahem** události a **souvislosti** s jinými událostmi (např. velký amplifikační DoS útok).
- Velkou roli také hraje **důležitost/role** cíle útoku (zařízení/služby).
  - **Jste ochotni poskytnout tuto informaci?**

Vizualizace

- Vhodně zobrazuje výstupy analýz pro dashboard
- Uvažované typy pohledů:
  - (Orientovaný) graf zachycující
    - souvislosti mezi událostmi,
    - agregované a komplexní události,
    - síťové rozsahy, příslušnost k doméně, AS atp.
  - Trendy - vývoj situace v čase – např. šíření botnetu
  - Počty/typy událostí na podkladové mapě

Dashboard

- Kontrolní panel pro správu systému SABU
- Centrální místo poskytující informace o všech komponentách
  - Výstup jednotlivých komponent
  - Stav systému – běží vše jak má?
- Jaké typy vizualizací poskytují osvědčené nástroje, které používáte?

Shrnutí

- iABU je komplexní komponenta SABU
- Budeme rádi za váš jakýkoliv podnět k:
  - Čističce – co čistit?, co teď prochází a nemělo by?
  - Vzorům pro analyzátor – jakým útokům čelíte?
  - Určování závažnosti – „vhledem“ do vaší sítě?
  - Způsobu obohacení – znáte další vhodný zdroj?
  - Vizualizaci a její využitelnosti – co (ne)funguje?
  - Obsahu dashboardu – co chybí, čeho je moc?