

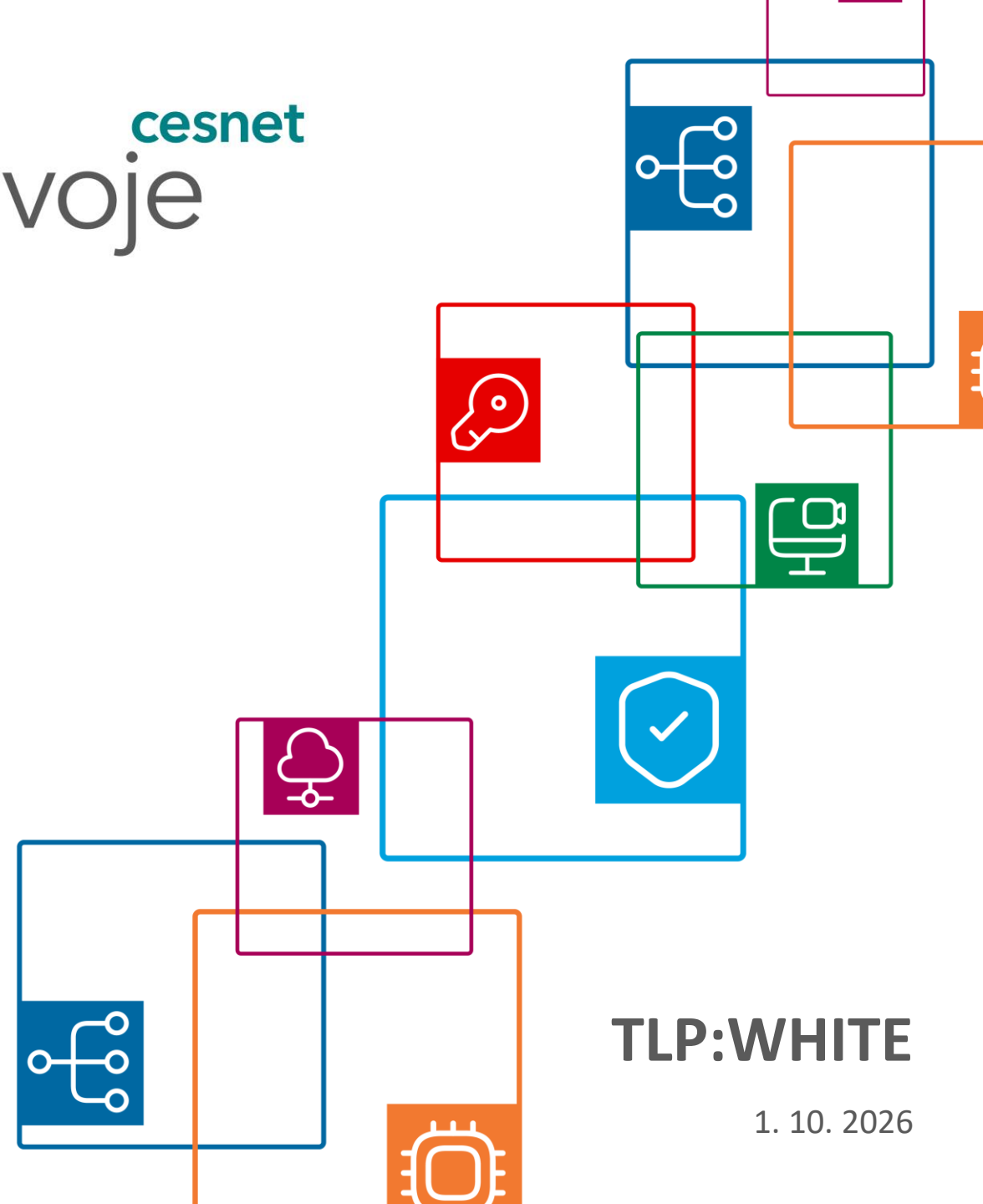


Metodická podpora pro logování v organizaci

Stanislav Špaček

Konference e-infrastruktury CESNET 2026

CSIRT-MU, Ústav výpočetní techniky, Masarykova univerzita



TLP:WHITE

1. 10. 2026

1. Metodická podpora pro logování v organizaci
(FR CESNET 2024/2025)
2. Řízení retence událostí podle legislativy
(FR CESNET 2026/2027)

- Co je to?
 - Protipól živelného přístupu – plánování, dokumentace, procesy
 - Příklady
 - Úvodní a průběžné stanovování rozsahu logování
 - Určení rolí stakeholderů
- Logování je v ČR legislativně regulované
 - nZKB, GDPR, jsme v souladu?
 - NÚKIB může provádět audity a udělovat sankce



■ Metodiky

- Soubory procesů, doporučení, a best practises pro provoz infrastruktury

■ Procesy

- Vývojový diagram
- Textový popis

■ Podpůrné materiály

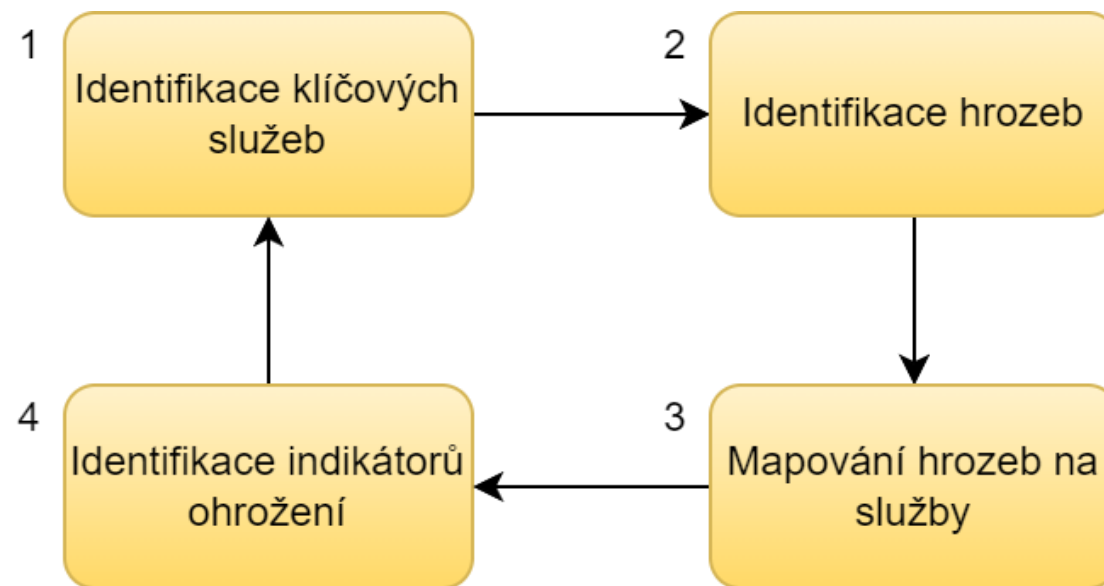
- Konfigurace běžných logovacích agentů
- Automatizace nasazení agentů (např. Ansible)



- **Zaměření logovací infrastruktury**
 - Určení rozsahu logování
 - Odhad nákladů logování
- **Vytvoření a údržba logovací infrastruktury**
 - Optimální nastavení logovací infrastruktury
 - Procesy pro běžné operace
- **Zpracování záznamu událostí**
 - Analýza dopadu zákonů platných v ČR na provoz logovací infrastruktury



- Jaké služby a jaké parametry optimálně logovat
- Příklad
 - Klíčová služba: Weby
 - Hrozba: Defacement
 - Indikátor ohrožení: Manipulace s obsahem webové stránky



- **Best practises pro provoz infrastruktury**
 - Zaznamenávání a interpretace času
 - Šifrovaný přenos událostí po síti
- **Procesy**
 - Přidání logování nové služby
 - Komunikace se stakeholdery
 - Monitorování infrastruktury
- **Dokumentace**
 - Knowledge base
 - Uživatelská příručka, FAQ



■ Jak dopadá na logování

- (Nový) Zákon o kybernetické bezpečnosti, 264/2025 Sb.
- Zákon o elektronických komunikacích, 127/2005 Sb.
- Nařízení o ochraně osobních údajů, GDPR 2016/679

■ Vymezená témata

- Jaké události a parametry mají být povinně logovány (NZKB, ZEK)
- Retence událostí (NZKB, ZEK, GDPR)
- Řízení přístupů (GDPR)

■ Konzultace konkrétních případů s právníky instituce je žádoucí



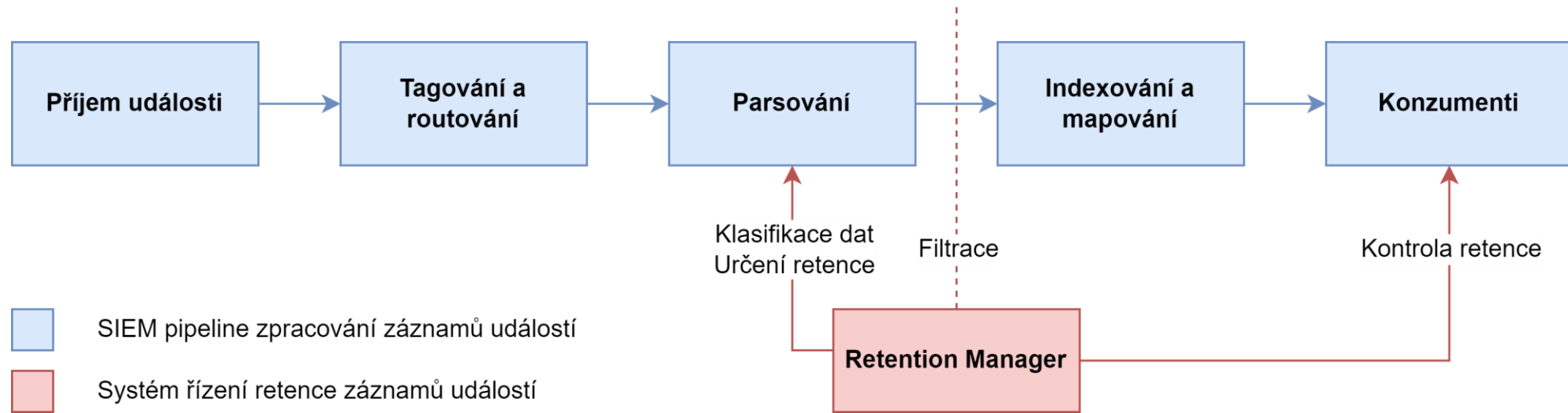
- **Infrastruktura**
 - Agenti (syslog-ng, rsyslog, *beat...) -> vector.dev -> OpenSearch, S3
- **Vývoj infrastruktury a řízení požadavků**
 - GitLab repositories + issues
- **Dokumentace**
 - GitLab, webová knowledge base interní a uživatelská
- **Procesy definované až na úroveň změn konfigurace (šablony)**
- **Přínosy**
 - Zalogování nové služby zkráceno z dnů na hodiny
 - Zapojení stakeholderů do vývoje infrastruktury
 - Odhaleno a vyřešeno několik konfliktů s legislativou



1. Metodická podpora pro logování v organizaci
(FR CESNET 2024/2025)
2. Řízení retence událostí podle legislativy
(FR CESNET 2026/2027)

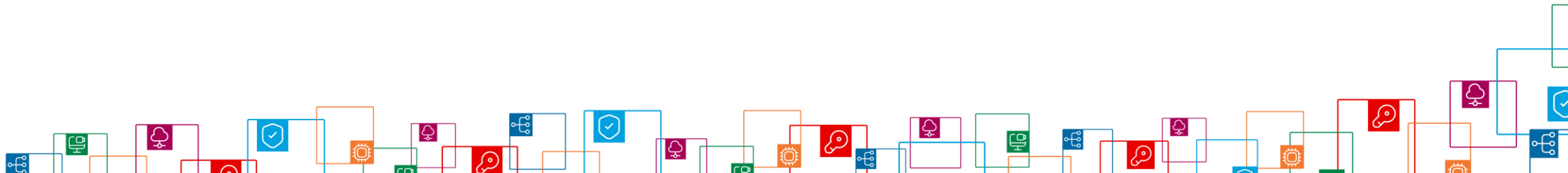
- **Řízení retence**
 - Efektivně, v souladu s legislativou, levně :)
- **Rozdělení komponent**
 - Systém řízení retence
 - Realizovaný v rámci existujícího SIEM
 - Transformace legislativy
 - „Naplnění“ systému konkrétními pravidly
 - Automatizace a asistence
 - Zefektivnění operací, minimalizace manuální práce



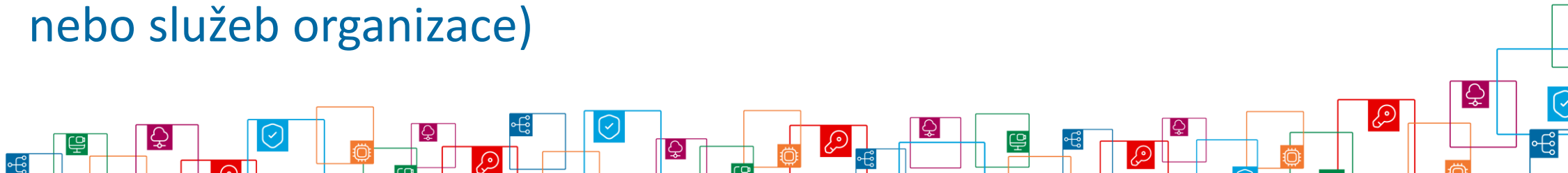


■ „Prostředek“ pro řízení retence

- Je nutné napojit do stávající infrastruktury a využít její funkce
- Udržet minimum vlastní implementace (ale všude se jí vyhnout nelze)



- „Mozek“ pro řízení retence
 - Vycházíme ze zákonů/vyhlášek, transformujeme na strojové direktivy
- Proces
 - Identifikovat všechny logované služby organizace (dokumentace)
 - Identifikovat zákony (analýza právních předpisů)
 - Identifikovat relevantní články
 - Mapovat články na služby
 - Vzniklou strukturu transformovat do nativních direktiv SIEM
- Proces manuální, mezioborový, a opakovaný (při změnách legislativy nebo služeb organizace)



- AI 😊
- Máme množství otázek k vyhodnocení
 - Lze použít naivní přístup?
 - Nakrmíme LLM model dokumentací a počkáme na výsledek
 - Jaké můžeme použít nám dostupné a open-source modely?
 - Např. CESNET, Ollama
 - Jsme schopni provádět automatizaci a asistenci lokálně?
 - Jak kvalitní a detailní dokumentace je třeba?
 - Zákony a vyhlášky jsou dané, ale co dokumentace organizace?



- **Systematizujte logovací infrastruktury**
 - Zrychlení provádění operací a nižší chybovost
 - Efektivnější komunikace mezi stakeholdery
 - Spolehlivější reakce na změny služeb a hrozeb
 - Možná kontrola souladu s legislativou
- **Do srpna 2027 pracujeme na systému řízení retence**
- **Popsané metodiky logování jsou veřejně dostupné jako výstupy projektu Fondu Rozvoje CESNET**
 - <https://is.muni.cz/publication/2509726/>

