2. schůze partnerů

SABU

20.6.2016

Program

- Zhodnocení dosavadních zkušeností se sdílením informací prostřednictvím mailového reportingu, Andrea Kropáčová
- Představení architektury systému SABU, Martin Žádník
- Návrh vstupně-výstupních konektorů, Pavel Kácha
- Obohacování dat, Martin Žádník
- Představení a popis iABU (komponenta systému SABU pro inteligentní analýzu událostí) - čistička, deduplikace, agregace, váhování, vizualizace, Jan Vykopal
- Systém NERD - Reputační databáze síťových entit, Martin Žádník
- Ukázka připojení Flowmon do systému Warden

Statistiky

Warden status


Database Size: 32.64 GB


Number of Events: 39342270


Number of Senders: 22


Number of Receivers: 27


Banner Created: 2016-06-20T09:00:01

Statistiky

	#reports	Reporting od
Casablanka	304	9.9.2015
ČDT	956	26.11.2015
O2	953	5.4.2016
ČSAS	0	6.4.2016
SANET	252	30.3.2016
GovCERT.CZ	2	Září 2015
Active24	5	Září 2015
Seznam	9	Leden 2015
DialTelecom	595	25.11.2015
CSIRT.SK		

Dojmy

- Data jsou užitečná pro sledování kondice sítě
- Změna šablon
- Změna interního work-flow CESNET-CERTS
- Změna typologie událostí?

Zapojení partnerů

- Odebírání dat
  - Přímo (konektor, vlastní zpracování, naskladnění a využití)
  - Formou e-mail reportu

- Zasílání dat
  - Provozujete bezpečnostní nástroj a jste ochotní data sdílet?
    - Jaká data?
    - Za jakých podmínek? Částečná anonymizace? Jen data relevantní pro CESNET2?
  - Máte vhodné místo v síti pro umístění nějakého bezp. nástroje?

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz