ISP – CyberCOP

Základní popis:
Systém je vhodný pro datová centra a poskytovatele internetu a obecně pro veškeré firmy, které potřebují chránit své počítačové sítě před napadením útočníky. Systém funguje tak, že analyzuje data procházející počítačovou sítí prostřednictvím sondy síťového provozu. Tato sonda předává informace o síťovém provozu s využitím protokolu IPFIX síťovým detektorům, které z poskytnutých dat odhalí základní typy síťových útoků jako např. port-scan, password cracking, DDOS, posílání spamu, atd. a reportují o tom správce sítě či uživatele. Systém je založen na platformě Apache Kafka určené pro zpracování velkých dat a umožňuje snadné a efektivní škálování systému.

Odlišnost od stávajících systémů:
Použití pokročilých metod strojového učení.
Orientace na platformu RouterOS, která je v praxi velmi často využívána, nicméně žádné komerční řešení obdobného charakteru na této platformě založené v současné době neexistuje.
Řešení vychází z praktických problémů, kteří řeší všichni ISP poskytovatelé.

Hlavní původce: Ing. Jan Fesl, Ph.D.

Jihočeská univerzita v Českých Budějovicích
Rektorát – Kancelář transferu technologií JU
Branišovská 1645/31a
CZ – 370 05 České Budějovice

Vyřizuje:
Ing. Veronika Štěpánová
T/ +420 389 032 025
E/ stepanova@jcu.cz
www.jctt.cz