Infraštruktúra pre riešenie kybernetických bezpečnostných incidentov a tvorbu datasetov

Vypracovala: Bc. Mária Činčuráková

Vedúci: Mgr. Jana Uramová, PhD.

ŽILINSKÁ UNIVERZITA V ŽILINE

Fakulta riadenia a informatiky

Katedra informačných sietí

Popis projektu

Datasety sú potrebné pre testovanie a trénovanie súčasných systémov pre detekciu prienikov do siete (útokov a anomálií), ale aj pre testovanie a trénovanie nových metód. V minulosti boli na fakulte nasadené nástroje pre detekciu útokov. Okrem týchto nástroj boli taktiež implementované aj nástroje pre archiváciu sieťových tokov pre online prevádzku a offline úložisko datasetov. Taktiež bola vypracovaná metodika pre celý proces riešenia kybernetických bezpečnostných incidentov.

Ciele projektu

Aktualizovať a zefektívniť proces riešenia kybernetických bezpečnostných incidentov a tvorby datasetov pomocou nasadených open-source nástrojov.

Doplnenie tzv. mobilnej sondy k aktuálne dostupných systémom Online a Offline Arkime.

Overenie vypracovanej metodiky pre tvorbu datasetov a ich značkovania.

Mobilná sonda

Hlavným dôvodom vytvorenia mobilnej sondy, je možnosť jej zapojenia do ľubovoľnej infraštruktúry, kde by identifikovala prieniky do infraštruktúry, archivovala prevádzku a upozornila na vznik bezpečnostných incidentov.

Aby sme sa na túto sondu vedeli pripojiť v prípade potreby, okrem spomenutých nástrojov sme využili aj nástroj OpenVPN, ktorý bude slúžiť na vzdialenú komunikáciu so sondou.

Použité nástroje

SURICATA

Arkime

elastic

kibana