Operačné centrum kybernetickej bezpečnosti (SOC) na KIS FRI UNIZA

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta riadenia a informatiky

Bc. Dominik Dvorský (dvorsky18@stud.uniza.sk)
Bc. Timotej Mačuha (macuha@stud.uniza.sk)

Projekt 3 - Aplikované sieťové inžinierstvo
Vedúci: Mgr. Jana Uramová, PhD.

Prečo SOC ?!

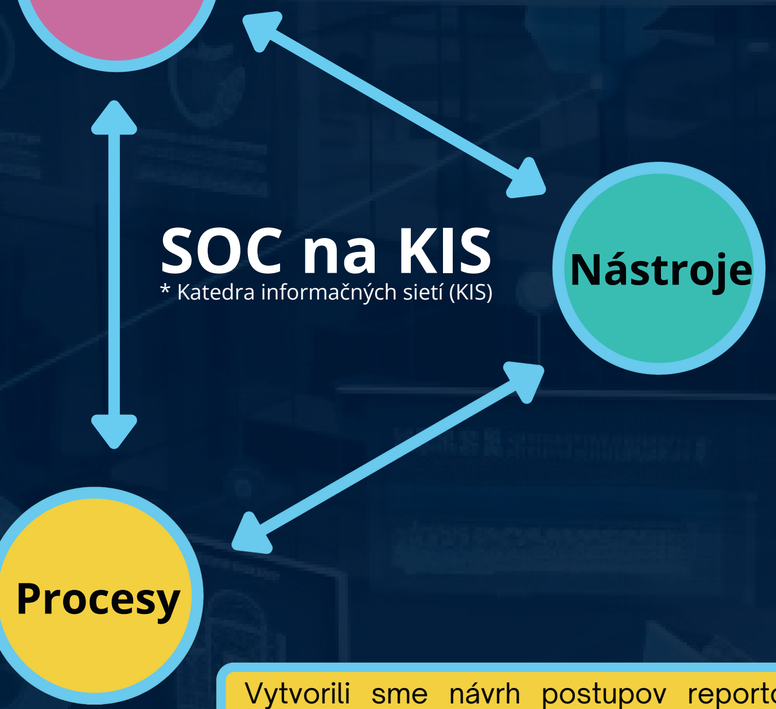
V súčasnosti je kybernetická bezpečnosť kľúčovou oblasťou informatiky, vzhľadom na neustále rastúci počet kybernetických útokov. S nárastom kybernetických hrozieb je nevyhnutné implementovať pokročilé bezpečnostné mechanizmy. SOC je práve takým mechanizmom. Jeho úlohou je monitorovať, detegovať, analyzovať a reagovať na kybernetické hrozby a útoky. Medzi jeho základné súčasti patria ľudia, procesy a nástroje.

Ciele do budúcna

Rozšírenie operačného centra kybernetickej bezpečnosti o ďalšie nástroje vrátane Threat Intelligence a procesy na zvýšenie ochrany. Implementácia monitorovania všetkých kritických služieb nasadených na fakulte, detekcia potenciálnych hrozieb a nastavenie efektívnych procesov na riešenie incidentov. Zlepšenie detekcie SOC emuláciou správania útočníka. Tieto kroky prispejú k ešte vyššiemu zabezpečeniu pred kybernetickými hrozbami a umožnia rýchlejšiu reakciu na nové útoky.

Dosiahnuté výsledky:

V projekte sme sa zamerali aj na prípravu ľudí pre prevádzku katedrového SOC. Na predmete RBI (Riešenie bezpečnostných incidentov) sme mali prednášku o skenovaní zraniteľností pomocou nástroja Greenbone a vytvorili sme zadanie a systém hodnotenia. Na základe toho vyberieme 3 najlepších študentov, ktorí dostanú ponuku pokračovať na Greenbone inžinierskom projekte. Tiež sme pripravili workshop pre SŠ.



Greenbone (OpenVAS): skener zraniteľností
Pripravili sme image** a nasadili ho na server. Skenovali sme podsiete na Fakulte riadenia a informatiky (FRI) a testovali rôzne nastavenia. O zraniteľnostiach sme informovali majiteľov zariadení a poskytli postupy na ich mitigáciu. Automatizovali sme odosielanie reportov do MS Teams pomocou Python skriptu a vytvorili ďalšie skripty na spracovanie a analýzu výstupov skenov. Na overenie zraniteľností sme generovali útočné skripty pre Metasploit pomocou Pythonu.

ELK (Elasticsearch, Logstasch, Kibana)
ELK-stack v našom projekte slúži ako nástroj pre riadenie bezpečnostných incidentov a udalostí (SIEM***). Nástroj sme správne nakonfigurovali a obnovili dashboardy, pre lepšiu vizualizáciu hrozieb v nástroji kibana. Nastavili sme mechanizmy pre detekciu potencionálne škodlivých aktivit v monitorovanej infraštruktúre. Navrhli sme vylepšenie nasadenia tohto nástroja.

** Obraz softvéru *** Security Information and Event Management

Vytvorili sme návrh postupov reportovania, schvaľovania, overenia mitigácie a akceptácie rizika a fromálne sme ich popísali v KIS Wiki dokumentačnom portáli.