EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

SPRÁVA A DOHLED NAD POČÍTAČOVOU SÍTÍ

Behaviorální analýza pomocí Flowmonu

Metodický list

Autor: Ing. Marek Kocan, Metodik: Bc. Jaroslav Tihlařík

Recenzent: Mgr. Jiří Činčura

Rok vydání: 2023

Obsah

Cíle

Studenti se seznámí s teoretickými základy v oblasti síťového monitoringu využitelného pro pokročilé – behaviorální – analýzy. Dále si osvojí základní dovednost ovládání jednoho z předních nástrojů této kategorie, ProgressFlowmon – konkrétně v rámci modulu Flowmon ADS. S ohledem na dotaci sice nelze předpokládat úplné zvládnutí tohoto nástroje, cílem je ale poskytnou studentovi dostatečný podklad pro orientaci v dané problematice.

Student bude schopen vlastními slovy vysvětlit co je síťový monitoring, bezpečnostní pohled na tuto oblast, pokročilé analýzy na základě chování i základní vlastnosti předvedeného produktu. V dlouhodobém horizontu bude student schopen samostatně po dalším doplnění využít nové znalosti a dovednosti v reálném prostředí pro odhalování problémů, detekci bezpečnostních incidentů a zvýšení všeobecného přehledu o konkrétní síťové infrastruktuře jako základního prvku ucelené podnikové informační architektury.

Současně je nicméně vhodné předřadit tomuto modulu výuku ProgressFlowmon obecně, nejde ale o nezbytnou prerekvizitu. Plusem je, pokud se student již orientuje v síťové problematice na úrovni RM ISO/OSI a TCP/IP včetně znalosti klíčových protokolů a principů IP adresace.

Dovednosti

Student bude schopen orientovat se v prostředí ProgressFlowmon, a to včetně provádění základních analýz včetně podrobného rozpadu. Dále bude student zvládat základní provázání s všeobecně dostupnými informacemi o síťové problematice (získané během studia na střední škole i během následné praxe) s cílem pochopit co nejvíce souvislostí o sledovaném prostředí.

Pracovní prostředí

Výuku lze realizovat v prostředí:

- Cylab JCEKB, ProgressFlowmon, modul ADS

Pro práci postačí standardní nástroje na klientském počítači – jakýkoli kompatibilní webový prohlížeč.

1 Síťový monitoring – teoretický základ

Síťová infrastruktura je dnes oprávněně považována za klíčovou součást jakékoli podnikové informační architektury, a to bez ohledu na vertikálu – tedy od školního prostředí přes oblast zdravotní péče nebo dopravu až například po moderní výrobní společnosti. Obdobné postavení pak v globální měřítku zaujímají rozlehlé sítě, a to včetně jejich nejznámějšího zástupce – internetu. Bez ohledu na použité technologie (v současnosti jde velmi často o sítě využívající tzv. TCP/IP stack) může během provozu nastat v síťovém prostředí celá řada typických i neočekávaných situací, provozního a bezpečnostního charakteru. Podobně lze nahlížet i na monitoring, tedy sledování sítí – z čistě provozního pohledu a z pohledu kybernetické bezpečnosti. Oba pohledy sice spolu souvisí, nicméně cíle obou oblastí jsou odlišné.

Provozní pohled souvisí především se zajištěním funkčnosti síťové infrastruktury, například pomocí detekce problémů a odhalení příčin atypických stavů. Jinými slovy, jde o zajištění každodenního provozu tak, aby mohli jednotliví zaměstnanci a systémy plnit své povinnosti. Bezpečnost souvisí s odhalením kybernetických incidentů na základě síťového provozu. Mezi základní možnosti patří odhalení pokusů o průnik skrze perimetr či přenos nakažených souborů. Všechny tyto tradiční metody mají jedno společné, a to že v menší či větší míře reaguji na známé vzory, například porovnávají předem známé signatury či upozorňují na určitý typ komunikace (například s potenciálně závadným cílem). Pokročilé mechanismy opřené dnes stále častěji i o prvky umělé inteligence posuzují skutečné dění na síti a na základě tzv. behaviorálních analýz (tedy analýz chování) odhalují i tradičními prostředky nedetekovatelné anomálie – například přenáší zaměstnanec větší objem dat než obvykle? Je ve výpovědní lhůtě? Bližší pohled ukáže, že komunikuje s dokumentovým serverem? A hned zde máme možnost odcizení firemní dokumentace. Mimochodem, toto je reálný a v praxi vyskytující se příklad, nikoli teoretická, nikdy nenastávající událost.

1.1 Flowmon ADS

Flowmon ADS je jedním z hlavních modulů produktu ProgressFlowmon – *vyučující dle svých znalostí vysvětlí pozadí vzniku této společnosti coby projektu v rámci vysokoškolského prostředí s následným komerčním úspěchem* – který patří mezi přední nástroje pro síťový monitoring (pojetí je mnohem širší, nicméně nad rámec výuky).

Jádro Flowmon ADS výrobce popisuje jako engine „využívající pokročilou analýzu chování k detekci nežádoucích anomálií v síťovém provozu. Dokáže odhalit nežádoucí chování, útoky na kritické aplikace, úniky dat a celou řadu indikátorů kompromitace.“. Dále pak uvádí, že Flowmon ADS přidává do bezpečnostní matice síťově orientovanou obrannou vrstvu, která odhalí i nepatrné síťové anomálie indikující aktivitu neznámých a vnitřních hrozeb, které nelze odhalit pomocí zabezpečení perimetru a koncových bodů. Přehledná vizualizace v rámci MITRE ATT&CK® frameworku následně informuje o rozsahu, závažnosti a dalším vývoji narušení.

V současné době se Flowmon ADS opírá o více než čtyři desítky detekčních metod založených na umělé inteligenci a o více než 200 sofistikovaných detekčních algoritmů. Díky tomu může odhalit také dosud neznámé hrozby zneužívající například i dosud nezveřejněné zranitelnosti.

2 Praktické ukázky ProgressFlowmon

2.1 Pracovní prostředí

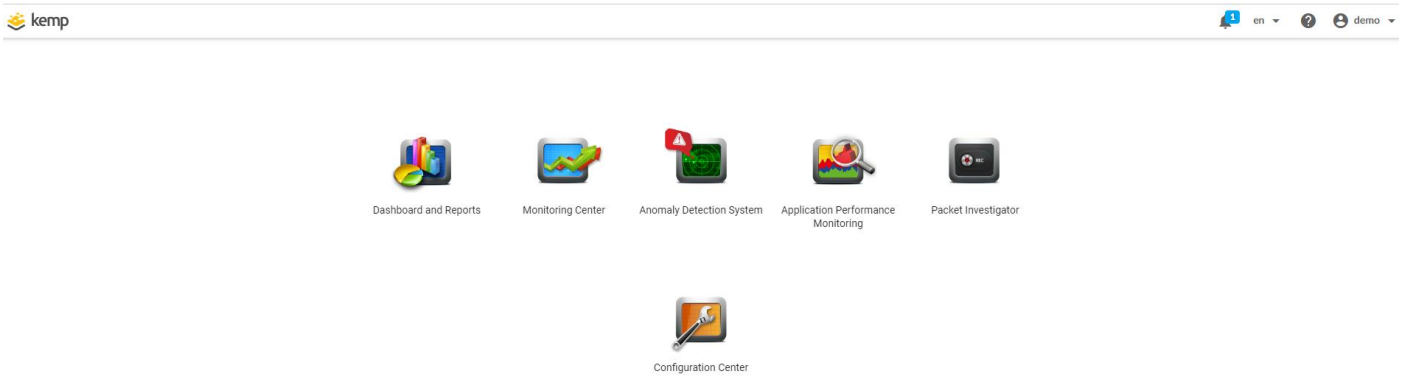
Výuku lze realizovat v prostředí Cylab JCEKB, ProgressFlowmon, modul ADS. Pro práci postačí standardní nástroje na klientském počítači – jakýkoli kompatibilní webový prohlížeč.

2.2 Přihlášení do systému

Vyučující seznámí studenty s teoretickými základy a následně předvede přihlášení do systému.

URL, uživatelské jméno a heslo: dle skutečného prostředí

Po úspěšném přihlášení je k dispozici základní rozcestník, například dle podoby na následujícím obrázku.



Vyučující vysvětlí dle svých znalosti jednotlivé moduly a ovládání (přepínaní jazyků a nápovědu).

Kontrolní bod

Studenti se přihlásí k ProgressFlowmon, přepnou si jazyk do češtiny a zobrazí si základní uživatelskou příručku. Následně si v rámci příručky zkusí najít informace o systémových požadavcích pro instalaci (cílem je ověřit schopnost pohybu po dokumentaci).

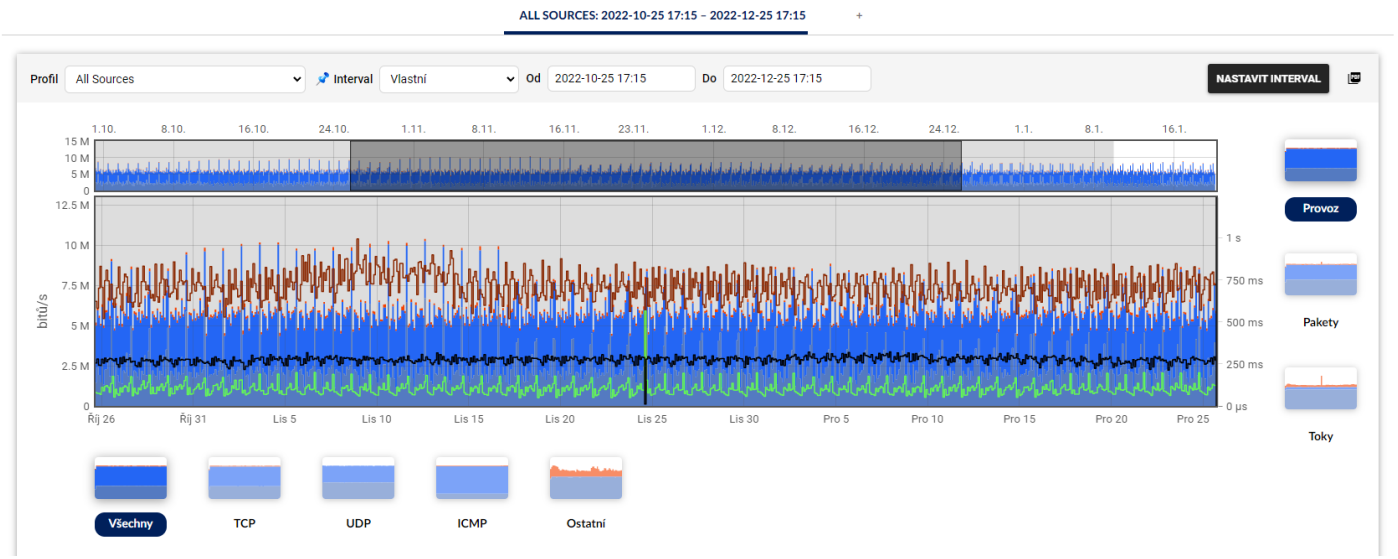
2.3 Monitoring Center

Monitoring Center je klíčovým modulem ProgressFlowmon a umožňuje základní i pokročilé analýzy sebraného síťového provozu. *Vyučující vysvětlí principy síťového monitoringu (technologie monitoringu síťových toků, zdroj dat – například sonda, kolektor). Vyučující může pro technický podklad vyjít například z popisu architektury v úvodu uživatelské příručky*

Vstup do monitorovacího centra je možný například pomocí klepnutí na ikonu Monitoring Center.

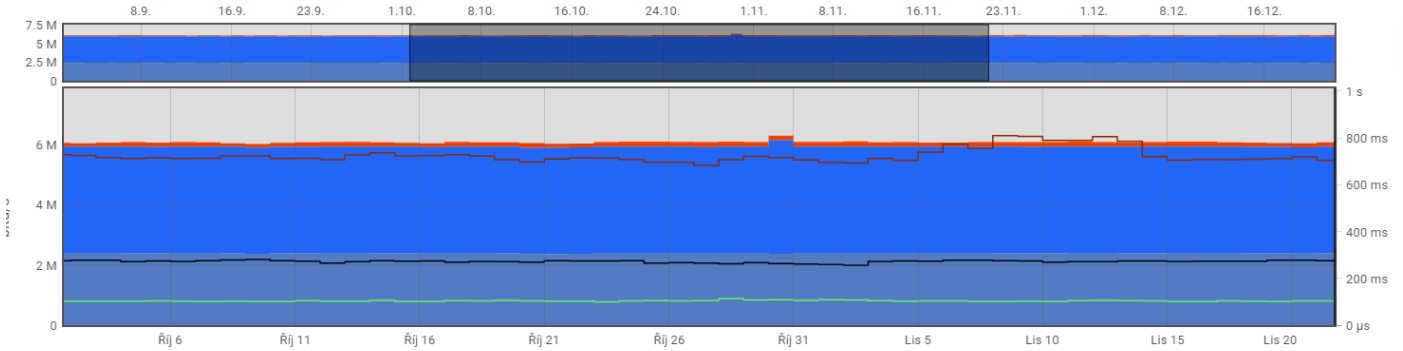
.

Součástí modulu je základní analytický přehled, který může dle nastavení vypadat například dle následujícího obrázku.



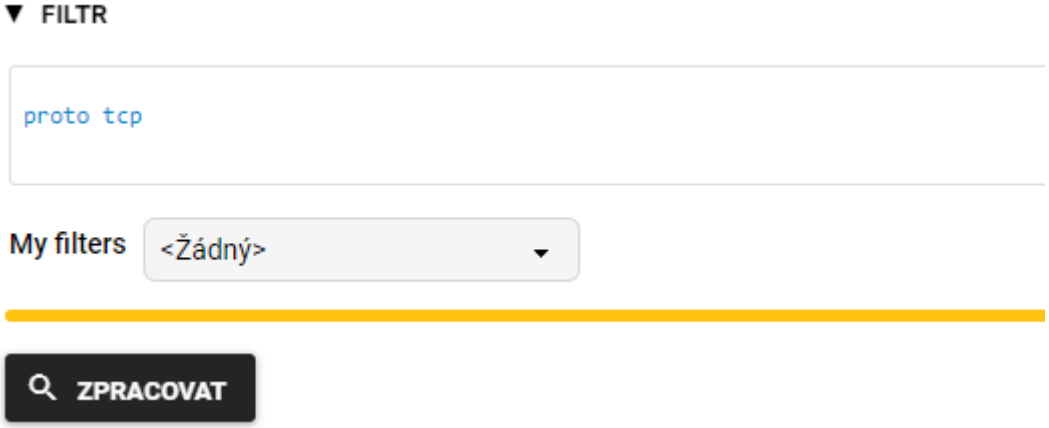
Profil zjednodušeně řečeno představuje předpřipravený zdroj dat, interval možnost ovlivnění časového okna dle přednastavených rozsahů nebo vlastní časový rozsah. Dále je možné filtrovat získané informace/statistiky dle základních protokolů (TCP/UDP/ICMP a ostatní), případně podle toho, zda jde o pakety nebo toky. *Vyučující vysvětlí – či v návaznosti na již proběhlou výuku síťových technologií vysvětlí – jednotlivé pojmy.*

Časový interval je možné nastavit nejen pomocí výběru, ale také interaktivním výběrem nad časovou osou/daty, například s tímto výsledkem (časy jsou vztažené k okamžiku pořízení snímků).



Vyučující předvede základní ovládání.

Další částí téže stránky je pokročilá analýza, umožňující filtrování dle zvolených kritérií, a to včetně pokročilých filtrů pomocí logických operátorů. Bližší popis je k dispozici v uživatelské příručce v kapitole 5.6 Syntaxe filtru.



Vyučující předvede filtr pro tcp a ukáže syntaxi pro ip adresu, například (dle příručky):

ip 192.168.2.4 - odpovídá konkrétní IP adrese (zdrojové i cílové).

src or dst ip 192.168.2.4 - je identický s předchozím.

src ip 192.168.2.4 - odpovídá konkrétní zdrojové IP adrese.

src host 192.168.2.4 - je identický s předchozím (IP a host jsou zaměnitelné).

proto tcp and (src ip 192.168.2.3 or dst ip 192.168.0.1) - odpovídá TCP komunikaci buď s první zdrojovou nebo druhou cílovou adresou.

Kontrolní bod

Studenti si vyzkouší základní práci v rámci modulu Monitoring Center a pomocí filtrů zkusí zjistit, zda se ve zvoleném časovém intervalu nachází nějaká síťová komunikace iniciovaná IP adresou 192.168.2.4 (IP adresu vyučující vhodně zvolí dle prostředí).

3 Praktické ukázky ProgressFlowmon ADS

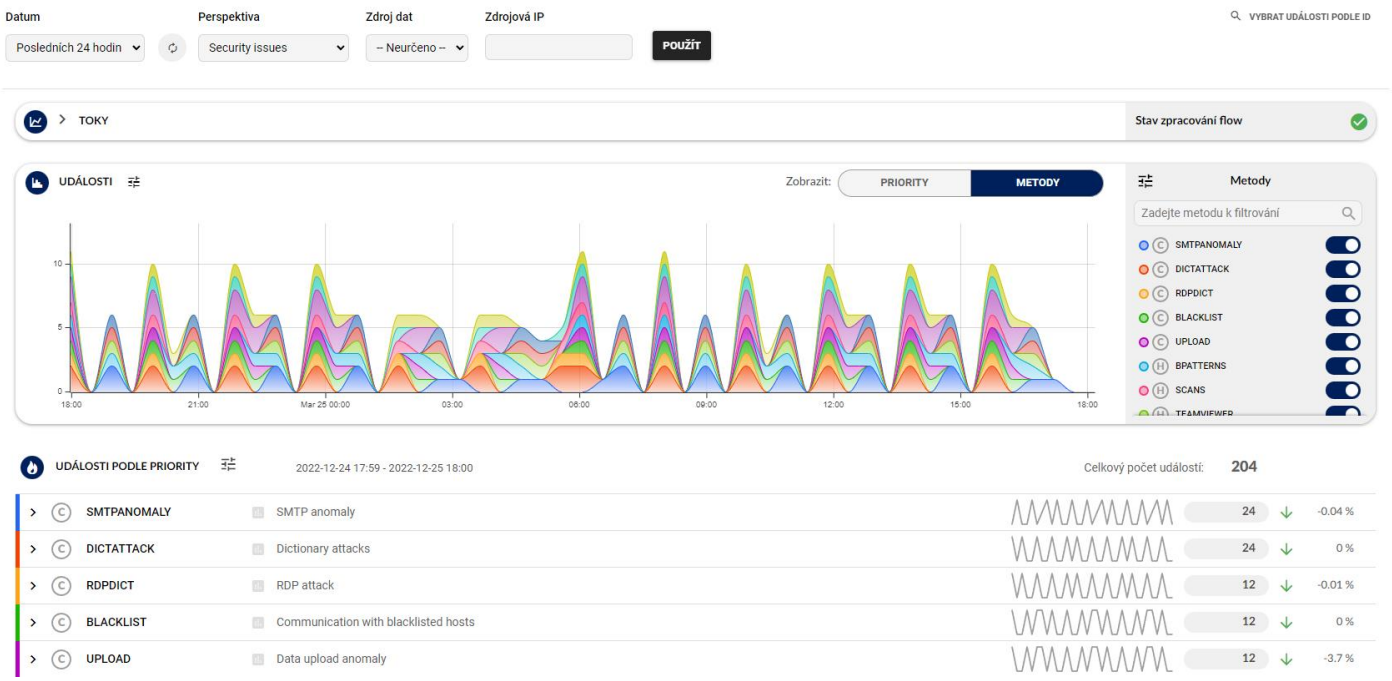
3.1 Vstup do modulu a základní ovládání

Vstup do ADS je možný například pomocí klepnutí na ikonu Anomaly Detection System.

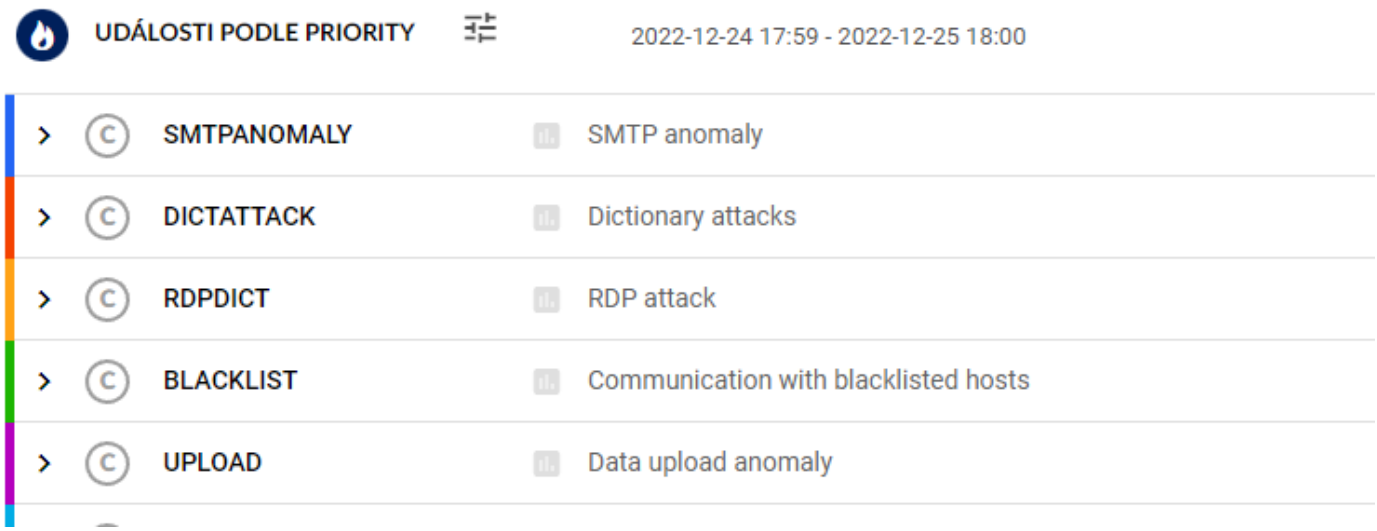
Anomaly Detection System

.

Součástí modulu je obdobný přehled, jako v případě monitorovacího centra, nicméně v tomto případě z bezpečnostního pohledu, jak je patrné z následujícího obrázku.



Vyučující předvede vstup do modulu ADS a upozorní na podobnost ovládání s monitorovacím centrem i na přehled událostí dle jednotlivých detekčních metod (v okamžiku výuky mohou být detekovány události podle jiných metod, na výše uvedeném obrázku jsou dle priority patrné metody SMTPANOMALY, DICTATTACK, RDPDICT ...).



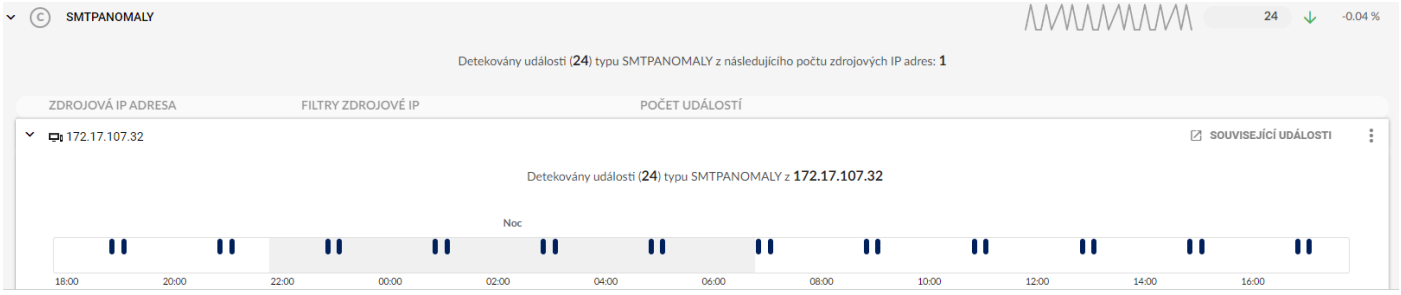
Dále vyučující upozorní na uživatelskou příručku, která se automaticky zobrazí pro modul ADS. Upozorní na kapitolu č. 3 s popisem detekčních metod. Se studenty probere dle své vlastní přípravy a dosavadních zkušeností vybrané metody.

Kontrolní bod

Studenti se přepnou do modulu ADS, shlédnou dle pokynu vyučujícího aktuální prostředí a v uživatelské příručce naleznou popis 1. zobrazené metody v analýze. Tuto metodu vzájemně s vyučujícím diskutují (pokud by byla na prvním místě vyučujícímu neznámá metoda, může se opřít o dokumentaci, případně zvolit jinou metodu).

3.2 Rozbor vybraného typu události

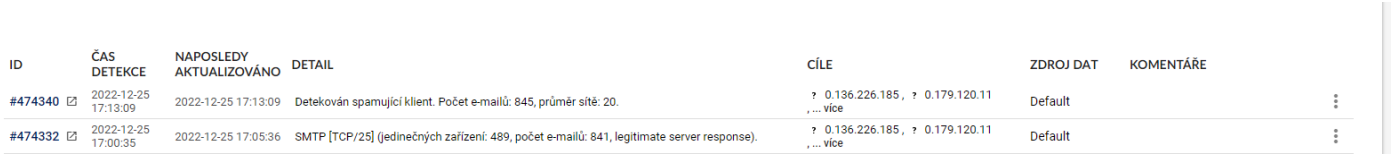
V analýze je možné postupně zjišťovat další informace o konkrétním typu události. V tomto scénáři budeme dále pokračovat s událostí typu SMTPANOMALY, kterou v základu uživatelská příručka popisuje jako „detekční metodu vycházející z předpokladu, že ve firemním prostředí by pošta měla být odesílána pouze definovaným způsobem. Metoda odhaluje odesílání nebo pokusy o odesílání mailů přes jiné než explicitně nadefinované poštovní servery.“. (Tento popis je pouze základním, vyučující by se měl podrobně s metodou v dokumentaci seznámit).



Zobrazení výše uvedeného detailu je možné docílit postupným rozkliknutím šipky u názvu typu události a IP adresy. Obrázek ukazuje zastoupení události v čase dle vybraného časového okna.

Vyučující předvede rozpad detailu události.

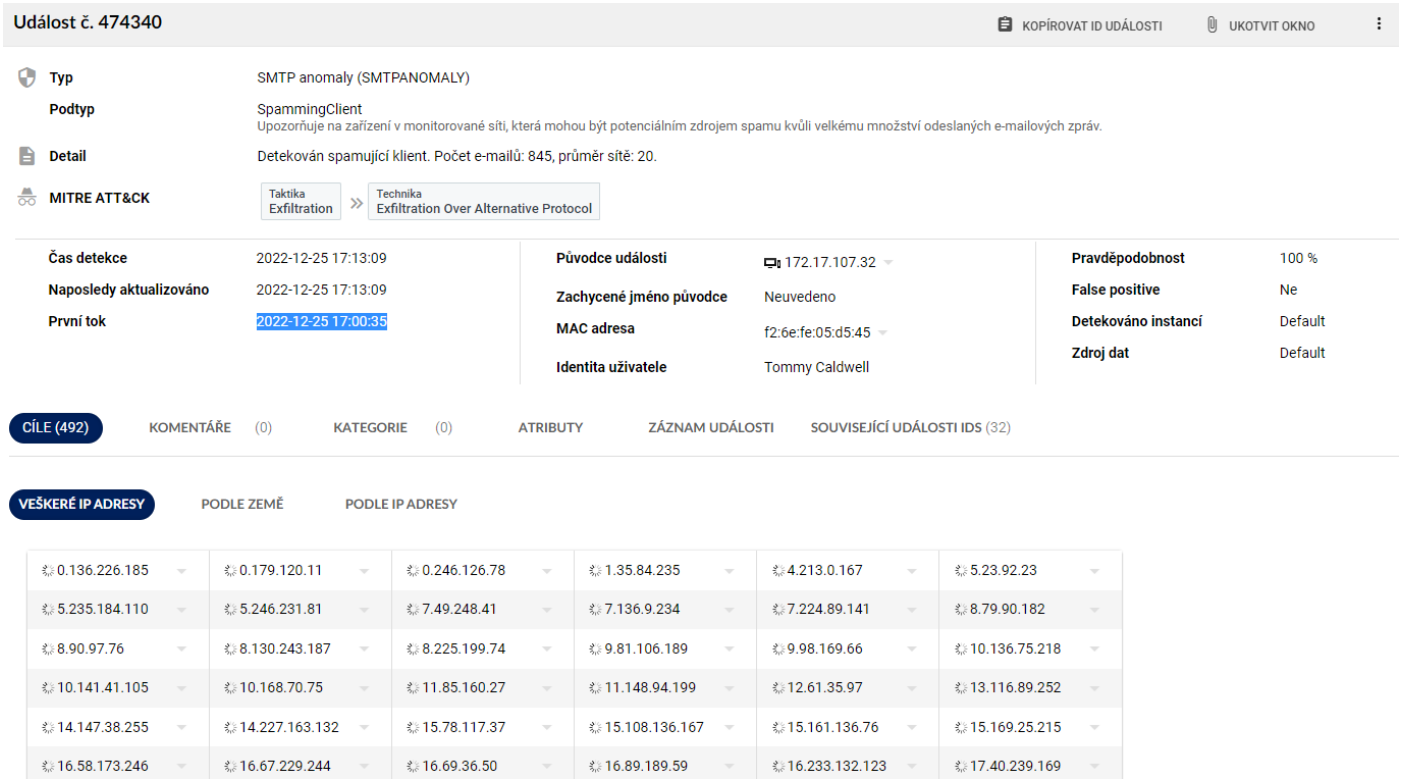
Součástí detailního seznamu získaného výše uvedeným postupem je i výpis jednotlivých událostí daného typu, například:



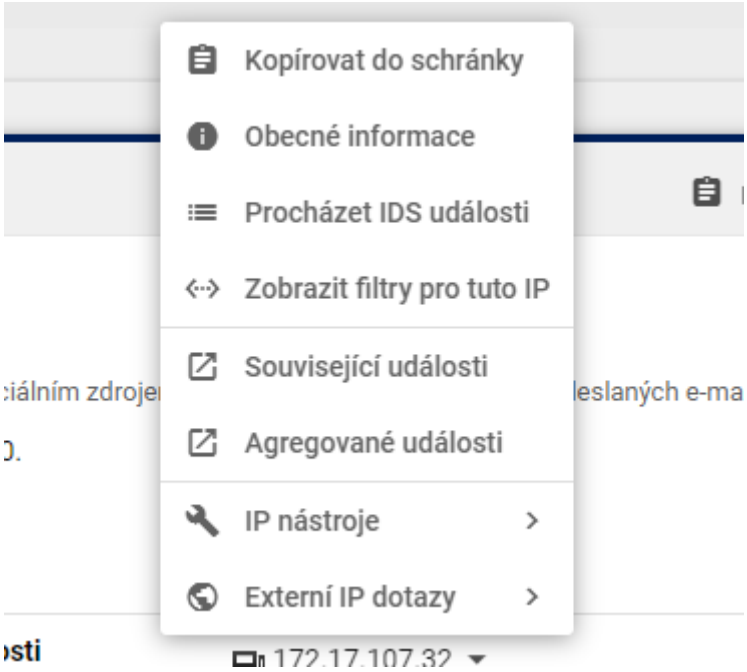
ID	ČAS DETEKCE	NAPOSLEDY AKTUALIZOVÁNO	DETAIL	CÍLE	ZDROJ DAT	KOMENTÁŘE
#474340	2022-12-25 17:13:09	2022-12-25 17:13:09	Detekován spamující klient. Počet e-mailů: 845, průměr sítě: 20.	? 0.136.226.185, ? 0.179.120.11, ... více	Default	
#474332	2022-12-25 17:00:35	2022-12-25 17:05:36	SMTP [TCP/25] (jedinečných zařízení: 489, počet e-mailů: 841, legitimate server response).	? 0.136.226.185, ? 0.179.120.11, ... více	Default	

Každá událost má své jedinečné referenční ID a v přehledu je zobrazena informace o času detekce, poslední aktualizaci na základě odpovídajícího zaznamenaného datového toku, detail události, cílech vztažených k události a zdroji dat.

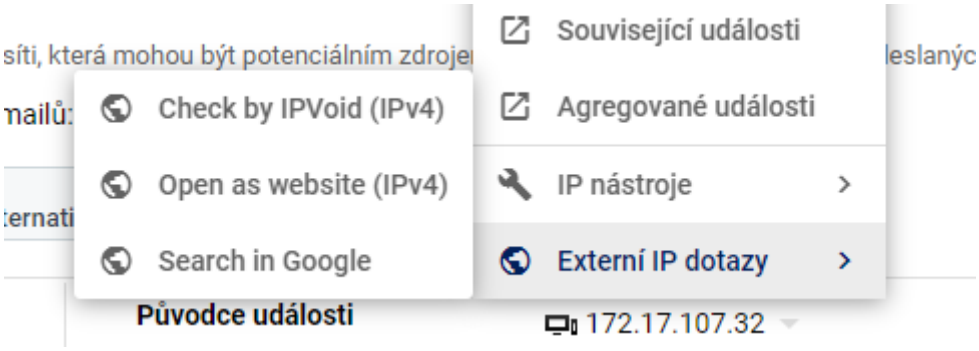
Po kliknutí na událost (ID) dojde ke zobrazení detailu dané konkrétní události – zde jsou obsažené podrobné informace včetně jednotlivých dotčených IP adres.



Na výše uvedeném obrázku je patrný původce události (172.17.107.32), užitečná je kontextová nabídka k ní vztažená umožňující další šetření:



Například externí IP dotazy do dalších systémů umožňujících ještě hlubší šetření:



Kontrolní bod

Studenti ve spolupráci s vyučujícím provedou detailní rozbor vybraného typu události v modulu ADS a pokusí se dohledat maximum souvisejících informací v monitorovacím centru.

Shrnutí a závěr

Studenti se seznámili se základním postupem využití ProgressFlowmon a modulu ADS včetně detailního rozboru jednoho konkrétního typu události. Dle svého uvážení může vyučující připravit pro studenty například praktický úkol nebo v případě větší časové dotace rozebrat další funkcionalitu, jako je nastavení jednotlivých meto, reporty nebo exporty do SIEM/nadřazeného prostředí.

Seznam použitých zdrojů

ProgressFlowmon. *Informace k produktu.* Dostupné z: https://flowmon.com