

Flowmon jako aktivní ochrana počítačové sítě

Bc. Matěj Fusek MBA



Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav krizového řízení

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Matěj Fusek, MBA
Osobní číslo:	L23020
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Rizikové inženýrství
Forma studia:	Kombinovaná
Téma práce:	Flowmon jako aktivní ochrana počítačové sítě

Zásady pro vypracování

1. Zpracujte teoretický vstup do řešené problematiky.
2. Analyzujte funkcionalitu nástroje Flowmon v reálném prostředí.
3. Realizujte aktivní ochranu počítačové sítě za pomoci nástroje Flowmon.
4. Navrhněte doporučení z hlediska implementace nových a úpravy stávajících funkcí nástroje Flowmon.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. COLLINS, Michael. *Network security through data analysis: from data to action*. 2nd ed. Beijing: O'Reilly Media, 2017. ISBN 978-1-491-96284-8.
2. Flowmon. *Detekce neznámých hrozeb*. Online. Brno: Flowmon, 2025 [cit. 2025-03-03]. Dostupné z: <https://flowmon.com/cs/solutions/security-operations/unknown-threat-detection>.
3. Flowmon. *Monitorování NetFlow / IPFIX*. Online. Brno: Flowmon, 2025 [cit. 2025-03-03]. Dostupné z: <https://www.flowmon.com/cs/solutions/network-and-cloud-operations/netflow-ipfix>.
4. KOLOUCH, Jan. *CyberSecurity*. Edice CZ.NIC. 2019. ISBN 978-80-88168-31-7.
5. ZHANG, Tianzhu; LINGUAGLOSSA, Leonardo; GALLO, Massimo; GIACCONE, Paolo a ROSSI, Dario. *FlowMon DPDK: Par-simonious Per-Flow Software Monitoring at Line Rate*. In: *2018 Network Traffic Measurement and Analysis Conference (TMA)*. 2018. ISBN 978-1-5386-7152-8.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **2. prosince 2024**
Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 24. dubna 2025

.....
podpis autora

ABSTRAKT

Tato diplomová práce se zaměřuje na analýzu, implementaci a vyhodnocení síťového monitorovacího systému Flowmon v akademickém prostředí Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Pozornost je věnována především schopnostem platformy Flowmon při detekci síťových hrozeb, anomálií a optimalizaci provozu univerzitní sítě. Práce zahrnuje popis architektury univerzitní sítě, metodiku nasazení Flowmonu a jeho klíčových modulů, zejména Monitoring Center a Anomaly Detection System (ADS). Na základě provedených testů a analýz jsou identifikovány silné i slabé stránky řešení, přičemž jsou navržena konkrétní opatření pro zlepšení bezpečnosti a výkonu sítě. V závěru práce jsou shrnuty přínosy systému Flowmon pro univerzitní prostředí a formulována doporučení pro další vývoj a rozšíření funkcionalit.

Klíčová slova: Bezpečnost, detekce hrozeb, Flowmon, kybernetický prostor, optimalizace sítě, síťové monitorování.

ABSTRACT

This thesis focuses on the analysis, implementation, and evaluation of the Flowmon network monitoring system in the academic environment of the Faculty of Logistics and Crisis Management at Tomas Bata University in Zlín. Particular attention is paid to the capabilities of the Flowmon platform in detecting network threats, anomalies, and optimizing performance within the university network. The thesis includes a description of the university network architecture, the methodology of deploying Flowmon and its key modules, particularly Monitoring Center and ADS. Based on the tests and analyses conducted, strengths and weaknesses of the solution are identified, and specific measures are proposed to improve network security and performance. In conclusion, the benefits of the Flowmon system for the university environment are summarized, along with recommendations for further development and enhancement of its functionalities.

Keywords: Cyberspace, Flowmon, network monitoring, network optimization, security, threat detection.

Na tomto místě bych rád poděkoval vedoucímu své diplomové práce **Ing. Petru Svobodovi, Ph.D.** za odborné vedení, cenné rady, trpělivost a podporu, které mi poskytl v průběhu zpracování této práce.

Zvláštní poděkování patří mé rodině, zejména manželce **Sabině**, která mi byla nepostradatelnou oporou a bez její trpělivosti, podpory a povzbuzení bych studium zvládal jen těžko. Děkuji také naší dceři **Beátě**, která mě svou přítomností motivovala pokračovat dál a babičkám **Jitce a Lence**, které nám nezištně pomáhaly nejen s hlídáním dcery, čímž nám umožnily úspěšně dokončit studium.

V neposlední řadě děkuji všem, kteří mi jakkoliv pomohli při tvorbě této diplomové práce – ať už odbornou konzultací, technickou pomocí, nebo morální podporou.

OBSAH

ÚVOD.....	10
CÍLE A METODY.....	12
I TEORETICKÁ ČÁST.....	13
1 ÚVOD DO PROBLEMATIKY POČÍTAČOVÉ BEZPEČNOSTI	14
1.1 NEJČASTĚJŠÍ KYBERNETICKÉ HROZBY	14
1.2 ZÁKLADNÍ KONCEPTY SÍŤOVÉ BEZPEČNOSTI	17
2 MONITOROVÁNÍ A ANALÝZA SÍŤOVÉHO PROVOZU.....	18
2.1 VÝVOJ METOD MONITOROVÁNÍ SÍŤOVÉHO PROVOZU	18
2.2 PŘÍSTUPY K MONITOROVÁNÍ SÍŤOVÉHO PROVOZU: AKTIVNÍ VS. PASIVNÍ METODY	19
2.3 TECHNOLOGIE POUŽÍVANÉ PRO ANALÝZU SÍŤOVÉHO PROVOZU	19
2.4 VÝHODY A NEVÝHODY RŮZNÝCH PŘÍSTUPŮ K MONITOROVÁNÍ SÍŤOVÉHO PROVOZU	20
3 FLOWMON – PŘEHLED TECHNOLOGIE	22
3.1 FLOWMON V KONTEXTU AKTIVNÍ OCHRANY SÍTÍ.....	24
3.2 SROVNÁNÍ FLOWMONU S JINÝMI BEZPEČNOSTNÍMI ŘEŠENÍMI	28
3.3 BUDOUCNOST A VÝVOJ FLOWMONU	32
3.4 REGULACE A LEGISLATIVNÍ POŽADAVKY NA MONITOROVÁNÍ SÍTÍ	35
4 SHRUTÍ TEORETICKÉ ČÁSTI.....	36
II PRAKTICKÁ ČÁST.....	38
5 ANALÝZA FUNKCIONALITY NÁSTROJE FLOWMON V REÁLNÉM PROSTŘEDÍ.....	39
5.1 FLOWMON MONITORING CENTER	50
5.2 FLOWMON ADS	67
6 NÁVRHY NA ROZVOJ A ÚPRAVY FUNKCIONALIT NÁSTROJE FLOWMON.....	81
6.1 MOŽNOSTI ROZŠÍŘENÍ FUNKCIONALITY	87
6.2 VYLEPŠENÍ UŽIVATELSKÉHO ROZHRAŇÍ A PŘÍSTUPNOSTI SYSTÉMU	96
ZÁVĚR	111
SEZNAM POUŽITÉ LITERATURY.....	113
SEZNAM OBRÁZKŮ	115
SEZNAM TABULEK.....	116
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	117

ÚVOD

V současné době představuje kybernetická bezpečnost jednu z nejvýznamnějších výzev pro správce sítí a organizace napříč celým spektrem odvětví. Neustálý růst množství přenášených dat, rozšiřování síťové infrastruktury a stále sofistikovanější metody kybernetických útoků kladou stále vyšší nároky na efektivní zabezpečení počítačových sítí. Problematika kybernetické bezpečnosti se již dávno neomezuje pouze na ochranu důvěrných informací a provozních systémů, ale zasahuje i do oblastí, jako je zajištění integrity a dostupnosti služeb, dodržování právních předpisů a standardů či ochrana proti průmyslové špionáži.

S rostoucím důrazem na proaktivní ochranu infrastruktury se stále častěji využívají technologie, které umožňují detekovat hrozby a anomálie v síťovém provozu na základě analýzy tokových dat. Mezi tyto technologie patří i systém Flowmon, který představuje moderní nástroj pro monitorování a analýzu síťového provozu s využitím pokročilých detekčních metod, jako jsou behaviorální analýza nebo strojové učení. Flowmon umožňuje efektivní detekci neznámých hrozeb, identifikaci anomálií a poskytuje přehled o chování celé síťové infrastruktury.

Tato diplomová práce se zaměřuje na nasazení a zhodnocení systému Flowmon v prostředí počítačové sítě Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Práce vychází z reálného provozu univerzitní sítě a zabývá se nejen analýzou schopností nástroje Flowmon v oblasti sledování provozu a detekce bezpečnostních incidentů, ale také návrhem konkrétních doporučení pro zlepšení funkčnosti systému v daném prostředí. Dílčím výstupem je posouzení účinnosti jednotlivých modulů a formulace návrhů na jejich optimalizaci, případně rozšíření funkcionality s ohledem na specifika univerzitní infrastruktury.

V teoretické části práce jsou uvedeny základní pojmy z oblasti kybernetické bezpečnosti, principy monitorování síťového provozu, technologie založené na analýze tokových dat a architektura systému Flowmon. Praktická část se věnuje samotnému nasazení systému Flowmon v akademické síti, jeho konfiguraci, sběru a analýze dat a vyhodnocení dosažených výsledků. Dále jsou prezentovány možnosti integrace Flowmonu s dalšími bezpečnostními nástroji a návrhy na zlepšení, která by mohla přispět k efektivnějšímu monitorování a ochraně síťové infrastruktury.

Výsledky práce poskytují nejen přehled o možnostech nástroje Flowmon v konkrétním akademickém prostředí, ale také obecné doporučení pro nasazení a optimalizaci podobných systémů v dalších organizacích. Vzhledem k rostoucím nárokům na kybernetickou bezpečnost a dodržování právních předpisů je zajištění efektivního monitorování a ochrany sítě zásadní pro udržení její stability, důvěryhodnosti a bezpečnosti.

CÍLE A METODY

Hlavní cíl

Posoudit funkcionalitu nástroje Flowmon pro potřeby aktivní ochrany počítačové sítě v akademickém prostředí a zhodnotit jeho efektivitu při detekci síťových anomálií a incidentů.

Dílčí cíle

1. Provést rešerši odborné literatury a analyzovat současné přístupy k monitorování síťového provozu a detekci kybernetických hrozeb.
2. Popsat architekturu a jednotlivé moduly systému Flowmon, včetně jejich schopností v oblasti monitorování a bezpečnostní analýzy.
3. Využít již nasazený systém Flowmon v univerzitní síti pro sběr a analýzu tokových dat s cílem ověřit jeho schopnosti v oblasti pasivního monitoringu a detekce anomálií.
4. Vyhodnotit účinnost detekčních mechanismů a možností automatizované reakce na bezpečnostní incidenty v prostředí univerzitní sítě.
5. Navrhnout konkrétní doporučení pro zlepšení funkcionalit systému Flowmon a jeho integrace do širšího bezpečnostního rámce akademické sítě.

Metody práce

V průběhu zpracování diplomové práce byly využity následující **vědecké metody**:

- **Analýza**

Byla využita jako stěžejní metoda této práce. Sloužila při rešerši odborné literatury, studiu dostupné dokumentace a technických specifikací systému Flowmon. Zároveň byla aplikována při vyhodnocení funkcionality systému v praxi, sledování a interpretaci výstupních dat z Flowmon Monitoring Center a Flowmon ADS.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY POČÍTAČOVÉ BEZPEČNOSTI

V současnosti je informační technologie neoddělitelně spjata s téměř všemi oblastmi lidské činnosti. Z toho důvodu je kybernetická bezpečnost považována za jedno z klíčových témat moderní digitální infrastruktury. S rostoucím množstvím přenášených dat, narůstající komplexitou sítí a zároveň vyšší intenzitou a promyšleností útoků, je stále větší důraz kladen na opatření, kterými je chráněna důvěrnost, integrita i dostupnost informací v digitálním prostředí (Stallings, 2020).

Počítačová bezpečnost bývá vymezována jako soubor technických, organizačních a procesních opatření, jimiž je zajišťována ochrana informačních systémů, síťových prvků a dat před neautorizovaným přístupem, narušením jejich funkčnosti nebo zneužitím. Vzhledem k neustále se měnící povaze hrozeb je vyžadována průběžná aktualizace bezpečnostních nástrojů i metodik, jinak může být prostředí snadno zranitelné. V praxi bývají nezabezpečené systémy často zneužívány k neoprávněnému přístupu, šíření malwaru, podvodným transakcím nebo dokonce k ovládání zařízení v rámci distribuovaných útoků (Schneier, 2021).

Kybernetické hrozby dnes ohrožují instituce všech velikostí a oborů. Ekonomické dopady útoků jsou přitom každoročně rostoucí. Podle zprávy společnosti Cybersecurity Ventures (Morgan, 2022) se odhaduje, že do roku 2025 dosáhnou celosvětové škody způsobené kyberkriminalitou až 10,5 bilionu amerických dolarů ročně. Tato predikce pouze potvrzuje významnost investic do bezpečnosti informačních systémů napříč veřejným i soukromým sektorem. S ohledem na složitost a rychlost moderních útoků je stále častěji přistupováno k implementaci automatizovaných nástrojů, jimiž je zajišťováno kontinuální monitorování provozu, detekce anomálií a schopnost okamžité reakce (Gartner, 2023).

1.1 Nejčastější kybernetické hrozby

Současné kybernetické hrozby se vyznačují značnou rozmanitostí a dynamickým vývojem, v jehož důsledku je komplikováno jejich včasné odhalení a účinné potlačení. Z pohledu organizací i jednotlivců představují tyto útoky zásadní bezpečnostní riziko, které může mít jak provozní, tak i ekonomické či reputační dopady. Mezi nejčastěji zaznamenávané typy hrozeb patří především malware, phishing, útoky typu DDoS (Distributed Denial of Service), ransomware a tzv. pokročilé perzistentní hrozby (APT). Každá z těchto kategorií je spojena s odlišným typem zneužití zranitelností a používá specifické prostředky a techniky.

Pod pojmem malware je označován škodlivý software, který je navržen s cílem poškodit nebo získat kontrolu nad napadeným systémem. Tento pojem zahrnuje celou řadu škodlivých kódů – od tradičních virů přes trojské koně až po spyware, kterým bývá sledována aktivita uživatele a získávána citlivá data (Kaspersky, 2023). V posledních letech je zaznamenáván zejména nárůst tzv. ransomwaru, tedy typu malwaru, jímž bývají data uživatele zašifrována a výměnou za dešifrovací klíč je požadováno výkupné.

Dalším běžným typem útoku je phishing, který využívá psychologické manipulace a sociální inženýrství. Při těchto útocích bývají oběti přiměny k poskytnutí přístupových údajů nebo stažení škodlivého souboru. Útočníci často napodobují důvěryhodné instituce (např. banky, univerzity, IT oddělení) a využívají podvržené e-maily nebo webové stránky k oklamání uživatelů (Verizon, 2022).

Významnou hrozbou pro stabilitu služeb je rovněž DDoS útok, při němž bývá síťový nebo aplikační server zahlcen enormním množstvím požadavků. Tím je znemožněn přístup legitimním uživatelům a dochází k výpadkům služeb. Tyto útoky bývají často prováděny s využitím botnetů tvořených infikovanými zařízeními, jež operují bez vědomí uživatele (Cloudflare, 2023).

Závažnou kategorií představují také APT útoky, které jsou charakteristické vysokou mírou sofistikovanosti a dlouhodobým působením v cílovém prostředí. Tyto útoky bývají realizovány s cílem průmyslové nebo politické špionáže, získání přístupu k chráněným informacím či strategické infiltraci do systémů. Vzhledem ke své nenápadnosti a nízké intenzitě je jejich detekce značně náročná, a proto bývají považovány za jednu z nejnebezpečnějších forem kybernetické hrozby (ENISA, 2022).

S rostoucí závislostí na digitálních technologiích se předpokládá, že výskyt těchto hrozeb bude nadále narůstat a jejich sofistikovanost se bude dále zvyšovat. Z tohoto důvodu je kladen důraz na prevenci, včasnou detekci a přijetí komplexních bezpečnostních opatření.

Malware a jeho varianty

Pod pojmem malware je označován škodlivý software, jehož účelem bývá poškození, narušení nebo převzetí kontroly nad napadeným zařízením bez vědomí uživatele. Tato forma hrozby patří k nejrozšířenějším a zároveň nejvariabilnějším nástrojům kybernetických útočníků. Vzhledem k neustálému vývoji metod útoku i šíření bývá malware distribuován prostřednictvím infikovaných e-mailových příloh, podvržených softwarových balíčků nebo využitím zranitelností v neaktualizovaných systémech (Kaspersky, 2023).

Mezi nejčastěji se vyskytující formy malwaru patří tzv. počítačové viry, tedy kódy připojované k jinak legitimním souborům, které se šíří mezi zařízeními při spouštění infikovaných programů. Závažnější formou jsou tzv. trojské koně, které se tváří jako běžný software, ale obsahují skrytý škodlivý kód, jímž může být útočníkovi umožněn vzdálený přístup k systému. Bývá jimi otevírána zadní vrátka, přes něž lze obcházet standardní bezpečnostní mechanismy. Další typ malwaru tvoří tzv. spyware, tedy software sloužící k nenápadnému sledování aktivity uživatele, například zaznamenáváním stisknutých kláves (keylogging), pořizováním snímků obrazovky nebo přesměrováním síťové komunikace. Zvláštní a v posledních letech extrémně rozšířenou kategorií je ransomware, tedy typ malwaru, kterým jsou soubory oběti zašifrovány a jejich zpřístupnění je podmíněno zaplacením výkupného. Podle zprávy Europolu (2023) patří ransomware k nejzávažnějším kybernetickým hrozbám současnosti a je využíván nejen vůči jednotlivcům, ale i vůči firmám, nemocnicím nebo univerzitám, přičemž způsobuje výrazné finanční i provozní škody.

Phishing

Phishingové útoky bývají řazeny mezi techniky sociálního inženýrství, při nichž jsou oběti manipulovány k tomu, aby dobrovolně poskytly útočníkům citlivé údaje. Nejčastěji se jedná o přihlašovací informace, údaje z platebních karet či jiné osobní nebo interní informace. Tyto útoky bývají realizovány prostřednictvím podvodných e-mailových zpráv, falešných webových formulářů nebo SMS komunikace, které věrně napodobují oficiální vzhled a jazyk důvěryhodných institucí, jako jsou banky, univerzity nebo státní úřady. Schopnost útočníků přizpůsobit obsah útoku konkrétní cílové skupině výrazně zvyšuje jejich úspěšnost. Podle analýzy společnosti Verizon (2022) patří phishing dlouhodobě k nejčastějším příčinám úspěšného narušení informační bezpečnosti.

DDoS útoky

Při útocích typu DDoS bývá cílová služba nebo infrastruktura záměrně zahlcena nadměrným počtem požadavků, v důsledku čehož dochází k přetížení systému a následné nedostupnosti pro legitimní uživatele. Tato forma útoku je typicky prováděna pomocí tzv. botnetů, tedy rozsáhlých sítí kompromitovaných zařízení, která jsou pod kontrolou útočníka. Pomocí těchto zařízení bývá zorganizována souběžná a koordinovaná aktivita, jejímž cílem je narušení provozní dostupnosti konkrétní služby nebo infrastruktury. Podle analýz společnosti Cloudflare (2023) patří DDoS útoky mezi nejčastější formy narušení dostupnosti

služeb a v posledních letech bývají stále častěji zaměřovány i na veřejné instituce, zdravotnictví a vysoké školy.

Pokročilé perzistentní hrozby (APT útoky)

APT jsou označovány jako dlouhodobé a technicky vysoce propracované útoky, jejichž cílem bývá průnik do specifického cílového systému a jeho následné skryté monitorování nebo manipulace po delší časové období. Tyto útoky bývají realizovány s vysokou mírou trpělivosti a přesnosti a často jsou spojovány s aktéry podporovanými státem. V praxi bývají APT kampaně zaměřovány na vládní instituce, kritickou infrastrukturu, výzkumné organizace a nadnárodní korporace. Klíčovým rysem těchto útoků bývá jejich nenápadnost a schopnost vyhnout se tradičním detekčním metodám po dlouhou dobu. Podle zprávy společnosti FireEye (2023) je tento typ útoku považován za jednu z nejvážnějších bezpečnostních hrozeb v současném kybernetickém prostředí.

1.2 Základní koncepty síťové bezpečnosti

S rostoucí intenzitou kybernetických útoků byla navržena a implementována celá řada bezpečnostních mechanismů, jimiž je usilováno nejen o prevenci hrozeb, ale i o jejich včasnou detekci a adekvátní reakci. Moderní přístupy ke kybernetické bezpečnosti bývají koncipovány jako vícevrstvé strategie, které využívají kombinaci technologií, jako je monitorování síťového provozu, segmentace sítí, řízení přístupových práv či šifrování přenášených dat (Stallings, 2020).

Zvláštní důraz je kladen na monitorování síťového provozu, které umožňuje odhalovat podezřelé aktivity a identifikovat vzorce chování, jež by mohly signalizovat probíhající útok. Tento přístup bývá realizován s využitím technologií typu NetFlow nebo IP Flow Information Export (IPFIX), které poskytují podrobné informace o síťových tocích. Využitím těchto dat je umožněna detekce anomálií v komunikaci i v chování jednotlivých zařízení. Nástroje jako Flowmon umožňují nejen sběr tokových dat, ale i jejich automatizovanou analýzu pomocí předdefinovaných scénářů detekce a reakcí na identifikované bezpečnostní incidenty (Flowmon, 2023).

2 MONITOROVÁNÍ A ANALÝZA SÍŤOVÉHO PROVOZU

V digitálně propojeném prostředí, v němž jsou podnikové sítě a kritická infrastruktura vystavovány neustálému riziku kybernetických útoků, se monitorování síťového provozu zařadilo mezi klíčové nástroje pro zajištění bezpečnosti i udržení provozní efektivity. Vzhledem k rostoucímu objemu přenášených dat a zároveň zvyšující se míře sofistikovanosti útoků se ukázalo, že tradiční obranné prvky – jako jsou firewally nebo antivirová řešení – již nepostačují. Moderní bezpečnostní strategie proto kladou důraz na proaktivní přístup, jehož základní součástí je právě kontinuální sledování síťového provozu a včasná detekce anomálií, jež mohou být příznakem bezpečnostního incidentu (Stallings, 2020).

Díky tomuto přístupu může být umožněna identifikace podezřelých vzorců chování, analýza síťových toků i odhalování hrozeb, které by jinak mohly zůstat nepozorovány. Kromě přínosu v oblasti bezpečnosti přináší monitorování také významné provozní výhody – např. možnost optimalizace síťového výkonu, identifikace přetížených segmentů, sledování kvality poskytovaných služeb (QoS) nebo efektivní diagnostika poruch. Rostoucí význam tohoto typu sledování je podpořen rovněž zvyšujícími se regulačními a legislativními požadavky, které zavazují organizace k zavedení kontrolních a auditních mechanismů. Tyto požadavky vyplývají mimo jiné z evropské směrnice NIS2 nebo nařízení GDPR, které zdůrazňují potřebu schopnosti detekce, reakce a dokumentace bezpečnostních událostí v síťovém prostředí (ENISA, 2023).

2.1 Vývoj metod monitorování síťového provozu

Metody monitorování síťového provozu prošly v posledních desetiletích zásadním vývojem, který byl vyvolán nárůstem objemu přenášených dat, vyšší mírou sofistikovanosti kybernetických útoků a zaváděním nových síťových architektur. Zatímco v dřívějších etapách vývoje byly sítě monitorovány převážně manuálně prostřednictvím logovacích záznamů a základních metrik, moderní přístupy se opírají o automatizovanou analýzu síťových toků, behaviorální modely a algoritmy strojového učení (Bejtlich, 2020).

Rozvoj cloudových technologií a nárůst šifrované komunikace způsobil, že tradiční metody typu Deep Packet Inspection (DPI) ztrácejí na účinnosti, protože není možné provádět inspekci obsahu přenášených dat bez porušení jejich důvěrnosti. V reakci na tuto situaci byly vyvinuty metody, které místo obsahu analyzují metadata o síťovém provozu. Technologie jako NetFlow a IPFIX poskytují detailní informace o síťových tocích – např. IP adresy,

porty, množství přenesených dat a časy komunikace – a tím umožňují efektivní monitorování provozu i v případě šifrované komunikace (Flowmon, 2023).

2.2 Přístupy k monitorování síťového provozu: aktivní vs. pasivní metody

V rámci monitorování síťového provozu bývají využívány dva základní přístupy, které se liší zejména způsobem sběru dat a vlivem na samotný síťový provoz. Jedná se o aktivní a pasivní metody monitorování, přičemž jejich použití závisí na konkrétním účelu a charakteru sledovaného prostředí (McGregor, 2021).

Při aktivním monitorování jsou do sítě cíleně vkládány testovací pakety, na základě jejichž odpovědí bývají měřeny různé parametry provozu, jako je latence, propustnost, odezva nebo dostupnost síťových služeb. Tento přístup bývá často využíván při diagnostice výkonových problémů nebo při ověřování QoS. Mezi jeho hlavní výhody patří možnost přesně zaměřeného testování vybraných síťových funkcí. Jako nevýhoda bývá uváděna skutečnost, že tímto způsobem může být síť zatěžována dodatečným provozem, což může být problematické zejména v prostředích s omezenou šířkou pásma (Cisco, 2023).

Pasivní monitorování se oproti tomu zaměřuje výhradně na sledování již probíhajícího provozu, aniž by do něj jakýmkoli způsobem zasahovalo. Tato metoda je založena na dlouhodobém sběru a analýze síťových dat, díky čemuž umožňuje identifikaci neobvyklých vzorců komunikace a potenciálních bezpečnostních incidentů. V oblasti kybernetické bezpečnosti bývá pasivní přístup upřednostňován, protože umožňuje detekci útoků v reálném čase a zároveň poskytuje historická data pro forenzní analýzu. Jeho nevýhodou je však skutečnost, že nedokáže aktivně ovlivnit síťový provoz a plní primárně roli detekční (Bejtlich, 2020).

2.3 Technologie používané pro analýzu síťového provozu

V moderních monitorovacích systémech bývají pro sběr a analýzu síťových dat využívány různé technologie, které se odlišují způsobem zpracování informací, strukturou exportovaných dat i mírou zatížení síťových zařízení. Mezi nejrozšířenější technologie v této oblasti patří NetFlow, IPFIX a Sampled Flow (sFlow), které jsou nasazovány v závislosti na konkrétním typu infrastruktury a požadavcích na granularitu dat.

NetFlow, technologie původně vyvinutá společností Cisco, umožňuje sledování tzv. síťových toků, tedy komunikací mezi dvěma koncovými body. Pomocí NetFlow bývají

zaznamenávány údaje o zdrojových a cílových IP adresách, portech, použitých protokolech, objemu přenesených dat a délce trvání přenosu. Tento formát je navržen tak, aby byl efektivní při monitorování rozsáhlých sítí a bývá využíván především pro účely bezpečnostní analýzy, optimalizace provozu a forenzního vyšetřování incidentů (Cisco, 2023).

Standard IPFIX (IP Flow Information Export) představuje modernizovanou a standardizovanou podobu původního NetFlow. IPFIX rozšiřuje možnosti sběru dat o širší podporu síťových protokolů a specifických metadat, čímž umožňuje detailnější analýzu provozu. Vzhledem ke své flexibilitě bývá IPFIX nasazován v pokročilých bezpečnostních platformách, jako je například systém Flowmon, který díky této technologii poskytuje podporu pro analýzu anomálií, detekci útoků a správu síťového výkonu (Flowmon, 2023).

Na rozdíl od předchozích technologií využívá sFlow princip vzorkování, kdy jsou pro účely analýzy zpracovávány pouze vybrané pakety z celkového provozu. Tento přístup umožňuje snížení výpočetních nároků na zpracování dat a je obzvláště vhodný pro prostředí s vysokým síťovým zatížením. Výhodou sFlow je nízká režie na straně zařízení, nevýhodou však bývá nižší přesnost a menší množství dostupných detailních informací ve srovnání s NetFlow nebo IPFIX. Vzhledem k těmto vlastnostem bývá sFlow využíván zejména v datových centrech nebo páteřních sítích, kde je prioritou rychlé zpracování a nízká zátěž infrastruktury (McGregor, 2021).

2.4 Výhody a nevýhody různých přístupů k monitorování síťového provozu

Každý z přístupů k monitorování síťového provozu disponuje specifickými výhodami i omezeními, které určují jeho vhodnost pro konkrétní použití. Aktivní monitorování umožňuje cílené testování vybraných parametrů sítě, což usnadňuje diagnostiku problémů s konektivitou, měření dostupnosti služeb nebo ladění výkonnostních charakteristik. Za nevýhodu tohoto přístupu bývá považována skutečnost, že generovaný testovací provoz zatěžuje síťovou infrastrukturu, a to zejména v prostředích s omezenou šířkou pásma nebo vysokými nároky na propustnost (Cisco, 2023).

Oproti tomu pasivní monitorování poskytuje komplexní pohled na reálný síťový provoz bez přímého zásahu do jeho průběhu. Umožňuje dlouhodobou analýzu trendů, detekci anomálií a identifikaci bezpečnostních incidentů v reálném čase. Tento přístup je však omezen tím,

že nedokáže aktivně reagovat na vzniklé problémy ani ovlivnit tok provozu, protože plní především detekční a analytickou funkci.

Rovněž jednotlivé technologie pro sběr dat přinášejí odlišné přínosy a kompromisy. NetFlow a IPFIX umožňují podrobnou analýzu síťových toků a bývají proto preferovány pro účely bezpečnostního dohledu, auditování a forenzní analýzy. sFlow, založený na principu vzorkování, představuje řešení s nízkou režijní náročností, a proto je vhodný tam, kde je třeba minimalizovat dopad monitorování na výkon zařízení. Volba konkrétní metody závisí na požadované úrovni detailu, výpočetních možnostech a charakteru sledované sítě (Bejtlich, 2020).

3 FLOWMON – PŘEHLED TECHNOLOGIE

V současné oblasti kybernetické bezpečnosti je kladen stále větší důraz na monitorování síťového provozu, detekci anomálií a aktivní ochranu před různými formami bezpečnostních hrozeb. Jedním z nástrojů, který tyto požadavky efektivně naplňuje, je Flowmon, specializovaná platforma určená pro detailní sledování a analýzu síťového provozu. Tento systém je navržen tak, aby umožňoval identifikaci potenciálních bezpečnostních incidentů, optimalizaci výkonu sítě a detekci odchylek od běžného provozního chování, které mohou být indikací probíhajícího útoku.

Základní funkcionality systému Flowmon je postavena na technologii NetFlow/IPFIX, která slouží ke sběru tokových dat a jejich následné analýze v téměř reálném čase. Díky této technologii může být síťový provoz sledován s vysokou úrovní podrobnosti, což umožňuje identifikaci nestandardních vzorců komunikace. V případě zjištění anomálií může být vyvolána automatizovaná reakce, čímž je zajištěna rychlá reakce na hrozby bez nutnosti manuálního zásahu (Flowmon, 2023).

Historie a vývoj platformy Flowmon

Platforma Flowmon byla původně vyvíjena v rámci výzkumného projektu realizovaného na Masarykově univerzitě v Brně, kde byl kladen důraz na pokročilé metody monitorování síťového provozu a analýzy dat. Tento akademický základ dal vzniknout samostatné společnosti Flowmon Networks, která se od počátku specializovala na vývoj profesionálních nástrojů určených k detekci anomálií, správě síťového provozu a ochraně před kybernetickými hrozbami.

Od svého vzniku byla platforma Flowmon postupně inovována, přičemž do jejího vývoje byly integrovány moderní analytické přístupy, prvky strojového učení i mechanismy pro automatizovanou detekci hrozeb. V roce 2020 byla společnost Flowmon Networks akvírována firmou Progress Software, globálním poskytovatelem bezpečnostních a integračních řešení. Touto akvizicí byl vytvořen prostor pro širší technologickou integraci a rozšíření kompatibility Flowmonu s dalšími bezpečnostními nástroji (Progress, 2021).

Díky následnému rozvoji se Flowmon stal součástí uceleného portfolia nástrojů určených pro síťovou viditelnost, bezpečnostní monitoring a provozní optimalizaci. Mezi nové funkcionality patří například modul Flowmon ADS pro pokročilou detekci neobvyklého

chování nebo Flowmon DDoS Defender, který zajišťuje rychlou detekci a mitigaci útoků typu DDoS (Flowmon, 2023).

Architektura řešení Flowmon

Architektura platformy Flowmon je navržena jako modulární systém, který se skládá z několika klíčových komponent umožňujících sběr, zpracování, vizualizaci a analýzu síťového provozu. Mezi základní prvky patří senzory, kolektory a řídicí konzole, které společně tvoří jednotné prostředí pro monitorování a ochranu sítě.

Senzory Flowmon jsou fyzická nebo virtuální zařízení, která bývají nasazována přímo do síťové infrastruktury. Jejich hlavní funkcí je sběr tokových dat a metadat o síťové komunikaci. Tyto senzory podporují standardy jako NetFlow, IPFIX či sFlow, díky čemuž je zajištěna jejich interoperabilita s různými typy síťových prvků. Pomocí senzorů jsou získávány detailní informace o každém síťovém toku, včetně IP adres, portů, využitých protokolů, objemu přenesených dat a doby trvání komunikace (Flowmon, 2023).

Kolektory Flowmon slouží k centralizovanému zpracování a analýze dat, která byla senzory nasbírána. V těchto jednotkách dochází k uložení informací, jejich strukturování a vyhodnocení na základě detekčních pravidel. Kolektory umožňují automatizované vyhledávání anomálií, rozpoznávání bezpečnostních incidentů a klasifikaci provozních událostí pomocí předdefinovaných scénářů nebo metod strojového učení (Progress, 2021).

Nad těmito prvky je umístěna řídicí konzole, prostřednictvím níž je zajištěn přístup k jednotlivým modulům systému. Grafické uživatelské rozhraní Flowmon Monitoring Center poskytuje přehled o aktuálním stavu sítě, zobrazuje detekované incidenty a umožňuje správu bezpečnostních politik. Díky integraci všech komponent do jednoho centrálního prostředí je umožněna efektivní správa síťového provozu, rychlá reakce na bezpečnostní hrozby a podpora provozní optimalizace (Flowmon, 2023).

Klíčové funkce a moduly platformy Flowmon

Platforma Flowmon je tvořena sadou specializovaných modulů, jimiž je rozšiřována základní funkcionality systému o pokročilé analytické a bezpečnostní schopnosti. Tyto moduly umožňují efektivní detekci kybernetických hrozeb, vizualizaci provozu a automatizovanou reakci na incidenty. Mezi klíčové komponenty patří Flowmon ADS, Flowmon DDoS Defender a Flowmon Monitoring Center.

Modul Flowmon ADS je navržen jako pokročilý detekční systém, kterým je analyzováno chování síťových prvků a identifikovány odchylky od běžných vzorců. Tento přístup je realizován prostřednictvím behaviorální analýzy a technik strojového učení, jimiž jsou rozpoznávány neobvyklé aktivity, potenciálně škodlivé připojení a známky probíhajících útoků. Pomocí tohoto modulu je možné detekovat například ransomware, neoprávněné přístupy nebo tzv. laterální pohyb útočníka v rámci interní sítě (Flowmon, 2023).

Dalším klíčovým prvkem je Flowmon DDoS Defender, který je určen pro detekci a zmírnění útoků typu Distributed Denial of Service. Modul využívá pokročilou analýzu objemových a aplikačních anomálií a umožňuje v reálném čase identifikovat a zablokovat abnormální síťovou aktivitu. Flowmon DDoS Defender je schopen spolupráce s externími ochrannými prvky, jako jsou scrubbing centra nebo cloudové služby pro mitigaci útoků, čímž je zajištěna vícestupňová ochrana před výpadky služeb (Progress, 2021).

Flowmon Monitoring Center zastává roli vizualizační a řídicí konzole, která sjednocuje informace ze všech senzorů a modulů. Toto rozhraní poskytuje ucelený pohled na aktuální stav síťového provozu a umožňuje správu detekovaných událostí. Díky grafickému zobrazení síťových toků, pokročilému vyhledávání a integraci s externími bezpečnostními systémy (např. SIEM) je umožněna efektivní správa infrastruktury a vyšetřování incidentů. Monitoring Center dále podporuje generování automatizovaných reportů a usnadňuje správu bezpečnostních politik (Flowmon, 2023).

3.1 Flowmon v kontextu aktivní ochrany sítí

V důsledku rostoucí complexity a propracovanosti moderních kybernetických hrozeb přestávají tradiční bezpečnostní opatření, jako jsou firewally nebo antivirové programy, plnit roli dostatečné ochrany síťových infrastruktur. Útočné techniky se neustále vyvíjejí, a proto je nutné, aby byly bezpečnostní systémy schopny nejen pasivního monitorování, ale i aktivní reakce na vzniklé incidenty. Z těchto důvodů se do popředí dostává koncept aktivní ochrany sítí, jehož cílem je nejen včasná detekce hrozeb, ale i jejich automatizované zvládnutí v reálném čase.

V tomto kontextu je platforma Flowmon vnímána jako pokročilý nástroj, který umožňuje komplexní analýzu síťového provozu, detekci odchylek od běžného chování a okamžitou reakci na podezřelé události. Pomocí technologií jako behaviorální analýza a strojové učení bývá umožněno rozpoznání neobvyklých vzorců komunikace a identifikace potenciálních hrozeb, ještě než dojde k jejich plnému projevení nebo poškození systému (Flowmon, 2023).

Detekce hrozeb

Detekce bezpečnostních incidentů a síťových anomálií je v rámci platformy Flowmon zajišťována kombinací několika analytických metod. Základem této činnosti je sběr a analýza síťových toků prostřednictvím technologií NetFlow a IPFIX, jimiž jsou získávány podrobné informace o jednotlivých komunikacích v síti. Na základě těchto dat je umožněno sledování vzorců chování zařízení, objemů přenesených dat, IP adres a dalších metrik, které slouží k odhalování podezřelých aktivit (Flowmon, 2023).

Hlavním nástrojem pro detekci hrozeb je modul Flowmon ADS, jehož úkolem je odhalování odchylek od běžného síťového chování. Tento systém využívá především behaviorální analýzu, pomocí níž jsou sledovány komunikační vzorce jednotlivých uzlů a identifikovány potenciální bezpečnostní hrozby. Detekovány tak mohou být například útoky typu ransomware, malware infekce, pokusy o laterální pohyb v síti nebo aktivity související s DDoS útoky (Progress, 2021).

Kromě behaviorální analýzy bývají v rámci systému Flowmon nasazeny i techniky strojového učení, jimiž je umožněna detekce dříve neznámých hrozeb na základě odchylek v síťovém provozu. Tímto způsobem mohou být identifikovány i tzv. zero-day útoky, které nejsou zachyceny tradičními signaturami nebo heuristikami. Algoritmy strojového učení analyzují historická data a rozpoznávají neobvyklé změny ve vzorcích komunikace, čímž je zajištěna vyšší míra citlivosti a přesnosti detekce (FireEye, 2023).

Integrace s jinými bezpečnostními nástroji

Platforma Flowmon není koncipována jako izolované řešení, ale jako otevřený a rozšiřitelný systém, který může být snadno integrován do existujícího bezpečnostního prostředí organizace. Díky podpoře standardizovaných protokolů a Programovací rozhraní aplikace (API) bývá umožněna spolupráce s celou řadou bezpečnostních technologií, jako jsou firewally, IDS/IPS systémy, Security Information and Event Management (SIEM) platformy či nástroje pro správu zranitelností.

V případě integrace s firewally může být zajištěna automatizovaná reakce na detekované bezpečnostní události. Flowmon je schopen identifikovat podezřelý provoz nebo útoky a následně generovat bezpečnostní politiky, které jsou předávány do firewallu. Tímto způsobem může být útočník zablokován již v rané fázi incidentu, čímž se snižuje riziko šíření hrozby v rámci sítě (Cisco, 2023).

Napojení na SIEM systémy (Security Information and Event Management) umožňuje centralizovanou správu bezpečnostních událostí a korelaci dat z různých zdrojů. Platforma Flowmon je schopna exportovat detekované anomálie a incidenty do nástrojů jako Splunk, IBM QRadar nebo ArcSight, kde jsou následně kombinovány s dalšími logy a výstupy z bezpečnostních prvků. Tímto způsobem je zajištěna vyšší přesnost detekce a lepší kontext při vyhodnocování incidentů (McGregor, 2021).

Díky uvedeným integracím bývá umožněna automatizace celého procesu detekce a reakce na hrozby, čímž se výrazně zkracuje doba potřebná pro identifikaci incidentu a realizaci příslušných opatření. Flowmon tak přispívá k vyšší efektivitě bezpečnostních operací a ke zlepšení celkového stavu kybernetické ochrany organizace (Flowmon, 2023).

Zero Trust a jeho propojení s Flowmonem

Současné přístupy ke kybernetické bezpečnosti stále častěji vycházejí z konceptu Zero Trust, podle něhož není v síťovém prostředí považováno žádné zařízení ani uživatel za důvěryhodného, dokud není důvěryhodnost jednoznačně ověřena. Tento bezpečnostní model je založen na principech nepřetržitého ověřování, segmentace přístupu a detailního monitorování síťového provozu. Jeho cílem je minimalizovat pravděpodobnost kompromitace systému i v případě, že útočník získá přístup do vnitřní části sítě (Gartner, 2023).

V tomto architektonickém rámci sehraává systém Flowmon zásadní úlohu, protože umožňuje monitorování provozu nejen na perimetru sítě, ale také uvnitř organizace. Díky analýze síťových toků a implementaci behaviorálních algoritmů může být detekováno chování, které se odlišuje od standardních vzorců. Tímto způsobem je umožněna identifikace tzv. laterálního pohybu útočníků, kteří již síť infiltrovali a snaží se eskalovat oprávnění nebo rozšířit přístup k dalším systémům (Progress, 2021).

Systém Flowmon tímto způsobem naplňuje jeden z klíčových principů Zero Trust přístupu – trvalé ověřování a sledování vnitřní komunikace, a zároveň přispívá k včasné automatické reakci na identifikované bezpečnostní hrozby. Díky těmto schopnostem může být Flowmon nasazen jako součást širší bezpečnostní architektury založené na principu nulové důvěry.

Automatická reakce na incidenty

Jedním z nejvýznamnějších přínosů platformy Flowmon je schopnost automatizované reakce na bezpečnostní incidenty, která umožňuje rychlé omezení nebo úplnou eliminaci

škodlivých aktivit bez nutnosti manuálního zásahu administrátora. Tento přístup výrazně zvyšuje efektivitu obranných opatření a snižuje čas potřebný k reakci na vznikající hrozby.

V rámci platformy Flowmon bývá tato funkcionalita zajišťována především modulem Flowmon ADS, jenž je schopen po detekci anomálie automaticky spustit předdefinované reakce. Jednou z nejčastějších forem reakce bývá automatizované blokování útočníka prostřednictvím firewallu, kdy je na základě identifikovaného chování vytvořeno pravidlo, které okamžitě omezí přístup útočícího zařízení do sítě. Tento krok bývá realizován bez lidského zásahu a pomáhá minimalizovat šíření útoku v jeho počáteční fázi (Progress, 2021).

Další možností reakce je generování výstrah a notifikací, které jsou směřovány k administrátorům sítě prostřednictvím e-mailu, systémů typu SIEM nebo jiných komunikačních kanálů. Tímto způsobem je zajištěna rychlá informovanost odpovědných osob a zjednodušeno následné vyšetřování incidentu.

V případě detekce útoků typu DDoS může být systém Flowmon propojen se specializovanými scrubbing centry nebo cloudovými DDoS ochrannými službami. Tyto externí prvky následně přebírají zátěž útoku a odfiltrují škodlivý provoz ještě předtím, než dojde k zahlcení interní infrastruktury (Progress, 2021).

Díky těmto automatizovaným procesům může být významně zkrácena doba potřebná k reakci na incident, a zároveň bývají minimalizovány negativní dopady na provoz organizace, ať už v podobě výpadků, ztráty dat nebo reputační újmy (FireEye, 2023).

Možnosti nasazení ve firmách a institucích

Platforma Flowmon nachází uplatnění napříč různými typy organizací a sektory, a to jak v soukromé, tak veřejné sféře. Díky své flexibilitě, škálovatelnosti a kompatibilitě s běžně využívanými síťovými technologiemi může být systém efektivně nasazován v podnikových sítích, finančních institucích, poskytovatelském sektoru i v prostředí veřejné správy.

V rámci podnikových sítí bývá Flowmon využíván zejména pro účely monitorování síťového provozu, detekce bezpečnostních hrozeb a zajištění provozní kontinuity. Díky tomu je organizacím umožněno včasné rozpoznání kybernetických rizik a snížení pravděpodobnosti výpadků služeb. Vysoká míra síťové viditelnosti přispívá k efektivnímu řízení infrastruktury a zvyšuje celkovou odolnost vůči útokům (Flowmon, 2023).

V sektoru finančních služeb je Flowmon nasazován za účelem detekce podvodného chování, ochrany transakčních systémů a naplňování regulačních požadavků v oblasti ochrany dat.

Platforma poskytuje nástroje pro audit a forenzní analýzu síťového provozu, čímž organizacím umožňuje splnění přísných standardů jako PCI-DSS nebo GDPR. Vzhledem k citlivosti zpracovávaných dat je detekce anomálií a schopnost včasné reakce na incidenty považována za klíčovou (ENISA, 2023).

Ve veřejné správě a prostředí kritické infrastruktury bývá Flowmon využíván k ochraně systémů zdravotnictví, státní správy nebo energetiky, kde je kladen důraz na zachování dostupnosti služeb a ochranu před sofistikovanými útoky, včetně těch podporovaných státními aktéry. Platforma umožňuje detekci pokusů o průnik, sledování síťových toků a řízení incidentů v souladu s bezpečnostními směrnicemi, jako je například evropská legislativa NIS2 (ENISA, 2023).

3.2 Srovnání Flowmonu s jinými bezpečnostními řešeními

V oblasti síťové bezpečnosti bylo v průběhu let vyvinuto široké spektrum nástrojů, jejichž cílem je detekce hrozeb, monitorování síťového provozu a zajištění ochrany před kybernetickými útoky. V tomto kontextu je řešení Flowmon profilováno jako pokročilá platforma, která kombinuje analýzu síťových toků s behaviorální detekcí anomálií a schopností automatizované reakce na incidenty. Oproti tradičním systémům, jako jsou IDS/IPS, nebo konkurenčním řešením typu Cisco Stealthwatch či Darktrace, přináší Flowmon řadu výhod souvisejících s hloubkou analýzy i škálovatelností nasazení.

Zásadní rozdíly mezi Flowmonem a tradičními nástroji spočívají v přístupu k detekci hrozeb, způsobu sběru dat a úrovni integrace do širší bezpečnostní infrastruktury. U klasických systémů detekce průniků (IDS/IPS) bývá detekce založena primárně na signaturách a statických pravidlech. Tento přístup je efektivní při rozpoznávání známých hrozeb, avšak méně účinný v případě nových nebo sofistikovaných útoků, které neodpovídají předem definovaným vzorcům (Collins, 2017).

Oproti tomu je ve Flowmonu aplikována behaviorální analýza, která umožňuje detekovat odchylky od běžného provozního chování. Pomocí metod strojového učení bývají identifikovány i zero-day hrozby nebo pokusy o laterální pohyb v síti, které by tradiční systémy nemusely zachytit. Tímto způsobem je zajištěna vyšší flexibilita a přesnost detekce i v prostředích s vysokou dynamikou provozu (Flowmon, 2023).

Rozdíl v metodách detekce hrozeb oproti jiným systémům

Podle Koloucha (2019) se moderní metody detekce hrozeb stále více zaměřují na behaviorální analýzu a monitorování anomálií namísto tradičních přístupů založených výhradně na signaturách. Tento přístup umožňuje detekovat hrozby, které nejsou předem známy nebo nebyly zaznamenány v databázích signatur, což je zásadní zejména při ochraně proti zero-day útokům. Kolouch (2019) rovněž zdůrazňuje význam korelace dat z více zdrojů a aplikace strojového učení při detekci APT.

Zatímco tradiční systémy detekce a prevence průniků (IDS/IPS) jsou založeny na detekci hrozeb pomocí signatur známých útoků, v případě Flowmonu je aplikována behaviorální analýza a strojové učení, čímž je umožněno odhalování i těch útoků, které nejsou zachyceny v databázích signatur. Tento přístup umožňuje detekci tzv. zero-day hrozeb, jejichž existence nebyla dříve známa a proti nimž klasické signaturní systémy nejsou účinné (Flowmon, 2023).

Flowmon nepřistupuje k síťovému provozu jako ke sledu izolovaných paketů, ale analyzuje komplexní vzorce chování v komunikaci mezi zařízeními. Díky tomuto kontextovému pohledu bývá umožněno přesnější vyhodnocení událostí v síti a výrazné omezení falešně pozitivních detekcí. Tím je zároveň snížena zátěž na bezpečnostní týmy, které se nemusí zabývat vyhodnocováním vysokého počtu chybných poplachů, jak tomu často bývá u tradičních IDS systémů (FireEye, 2023).

Výsledkem tohoto přístupu je vyšší přesnost detekce a rychlejší reakce na skutečné incidenty, a to i v prostředích s vysokou variabilitou provozu, kde by statická pravidla selhávala.

Flowmon vs. tradiční IDS/IPS systémy

Systémy detekce a prevence průniků (IDS/IPS) představují dlouhodobě standardní součást síťové bezpečnosti a jsou nasazovány k identifikaci a blokování známých hrozeb. Tyto systémy fungují na principu analýzy síťového provozu s využitím předdefinovaných signatur, které umožňují rozpoznání známých útoků.

Flowmon se od tradičních IDS/IPS systémů liší tím, že nepracuje pouze se signaturami, ale využívá behaviorální analýzu síťového provozu, což mu umožňuje detekovat i dříve neznámé hrozby. Tento přístup je zásadní zejména v boji proti zero-day útokům, při nichž se útočníci snaží zneužít dosud neodhalené zranitelnosti systémů. IDS/IPS systémy jsou

schopny odhalit útoky pouze v případě, že odpovídají známým vzorcům chování, zatímco Flowmon dokáže identifikovat anomálie v síťovém provozu i bez znalosti konkrétního exploitu (Flowmon, 2023).

Dalším klíčovým rozdílem je způsob interakce s provozem v síti. IDS systémy jsou pasivní a pouze upozorňují na podezřelé aktivity, zatímco IPS systémy mají schopnost aktivně blokovat provoz na základě předdefinovaných pravidel. Flowmon se v tomto ohledu chová jako hybridní řešení, protože umožňuje nejen detekci hrozeb, ale také automatizovanou reakci, například prostřednictvím integrace s firewalley nebo jinými bezpečnostními systémy (Progress, 2021).

Další nevýhodou tradičních IDS/IPS systémů je vyšší míra falešných poplachů (false positives). Flowmon ADS naopak využívá kombinaci strojového učení a behaviorální analýzy, což snižuje počet falešných hlášení a zvyšuje přesnost detekce bezpečnostních incidentů (FireEye, 2023).

Výhody oproti jiným síťovým monitorovacím řešením

Vedle IDS/IPS systémů existuje na trhu řada dalších nástrojů určených k monitorování síťového provozu a detekci bezpečnostních hrozeb. Mezi významné konkurenty platformy Flowmon patří například Cisco Stealthwatch, Darktrace či řešení od Arbor Networks. Každý z těchto nástrojů nabízí specifické přístupy k analýze dat, reakci na incidenty i integraci do širší bezpečnostní architektury.

Cisco Stealthwatch je nástrojem zaměřeným na analýzu síťového provozu pomocí technologií NetFlow/IPFIX. Stejně jako Flowmon, i tento systém využívá behaviorální analýzu ke sledování síťových vzorců a detekci anomálií. Jeho hlavní nevýhodou však bývá silná závislost na Cisco ekosystému, což omezuje možnosti jeho nasazení v prostředích s různorodým hardwarovým vybavením. Naproti tomu je Flowmon navržen jako otevřené řešení, které podporuje široké spektrum standardizovaných protokolů, čímž je umožněna jeho bezproblémová integrace i do heterogenních infrastruktur (Cisco, 2023; Flowmon, 2023).

Darktrace přistupuje k analýze provozu pomocí umělé inteligence a hlubokých neuronových sítí. Jeho síla spočívá v adaptivním modelu učení, který umožňuje identifikaci složitých a neobvyklých anomálií. Na druhé straně je však tato technologie spojena s vyšší latencí při zpracování dat a vyššími nároky na implementaci i provozní rozpočet. Flowmon nabízí v tomto ohledu vyvážený kompromis mezi pokročilou detekcí a efektivitou provozu, což jej

činí vhodným i pro menší a středně velké organizace, které si nemohou dovolit komplexní AI řešení s vysokými náklady (Darktrace, 2023; Flowmon, 2023).

Oproti řešením od Arbor Networks, která se specializují výhradně na detekci a mitigaci DDoS útoků, poskytuje Flowmon komplexní bezpečnostní funkcionalitu. Kromě DDoS ochrany bývá umožněna také detekce malwaru, pokročilých síťových anomálií, a integrace s firewally, SIEM systémy a dalšími komponentami zabezpečení. Zatímco Arbor je ideálním nástrojem pro poskytovatele internetových služeb a velké podniky zaměřené na volumetrické útoky, Flowmon je vnímán jako univerzálnější platforma vhodná pro širší spektrum bezpečnostních potřeb (Progress, 2021).

Praktické zkušenosti a případové studie

Systém Flowmon byl úspěšně nasazen v celé řadě organizací napříč různými sektory, včetně podnikových sítí, finančních institucí, zdravotnických zařízení i veřejné správy. V těchto prostředích byla jeho efektivita opakovaně potvrzena, a to zejména v oblastech automatizované detekce hrozeb, zkrácení doby reakce na incidenty a ochrany kritické infrastruktury. Nasazení systému Flowmon bývá často doprovázeno snížením provozních rizik a zvýšením celkové odolnosti vůči kybernetickým útokům (Flowmon, 2023).

V jedné z případových studií byl systém Flowmon nasazen ve finanční instituci, kde bylo požadováno monitorování síťového provozu v reálném čase a identifikace podezřelých transakcí. Po implementaci bylo dosaženo výrazného snížení počtu neodhalených incidentů. Flowmon byl v tomto prostředí schopen identifikovat vzorce chování charakteristické pro podvodné aktivity, které by jinými nástroji zůstaly nepovšimnuty (Progress, 2021).

Úspěšná implementace byla zaznamenána také v oblasti zdravotnictví, konkrétně při ochraně nemocniční infrastruktury před ransomwarovými útoky. V tomto případě bylo Flowmonem zajištěno včasné rozpoznání hrozeb a následná reakce prostřednictvím integrace s firewally a SIEM systémy. Díky tomu byla zabráněna kompromitaci citlivých dat pacientů a přerušení poskytování zdravotnických služeb, což je v prostředí nemocnic kriticky důležité (ENISA, 2023).

Tyto případové studie potvrzují, že Flowmon nachází uplatnění nejen ve velkých podnicích, ale také v odvětvích, která vyžadují vysokou dostupnost služeb a zvýšené bezpečnostní nároky.

3.3 Budoucnost a vývoj Flowmonu

Dynamický vývoj kybernetických hrozeb klade stále vyšší nároky na efektivitu nástrojů síťové bezpečnosti. Moderní bezpečnostní systémy musí být schopny nejen monitorovat provoz, ale také aktivně detekovat a eliminovat bezpečnostní incidenty v reálném čase. Vzhledem k neustále rostoucímu objemu síťových dat a stále sofistikovanějším útokům se budoucnost těchto řešení spojuje především s automatizací, umělou inteligencí a pokročilými analytickými metodami (Gartner, 2023).

Platforma Flowmon se jako moderní nástroj pro analýzu síťového provozu a detekci anomálií neustále vyvíjí a přizpůsobuje aktuálním trendům v oblasti síťové bezpečnosti. Směry dalšího rozvoje zahrnují především využití umělé inteligence (AI), hlubší integraci s dalšími bezpečnostními systémy a rozšíření funkcionality směrem k automatizované kybernetické obraně (Flowmon, 2023).

Mezi klíčové oblasti budoucího rozvoje patří implementace pokročilých algoritmů strojového učení, které mají umožnit přesnější detekci neznámých hrozeb. Tento přístup bude zaměřen nejen na identifikaci anomálií v reálném čase, ale také na schopnost adaptivního učení a predikce budoucích útoků na základě historických dat. Přesnost detekce by tím měla být zvýšena i v prostředích s vysokou dynamikou provozu (Gartner, 2023).

Dalším důležitým aspektem rozvoje je rozšíření schopnosti integrace Flowmonu s ostatními bezpečnostními nástroji. Jedná se především o rozhraní s firewally, SIEM systémy, nástroji pro správu zranitelností a dalšími platformami, které umožňují centralizované řízení bezpečnostních incidentů. Automatizace reakce na detekované hrozby tím může být dále vylepšena, což přispěje k rychlejší eliminaci bezpečnostních rizik (Flowmon, 2023).

V neposlední řadě se budoucí vývoj Flowmonu zaměřuje na zlepšení uživatelské přívětivosti a efektivitu práce bezpečnostních týmů. Využití pokročilých analytických nástrojů, automatizovaných reportů a přehlednějšího uživatelského rozhraní má za cíl minimalizovat čas potřebný k identifikaci a řešení bezpečnostních incidentů. Díky těmto krokům by měl být Flowmon nadále schopen držet krok s vývojem kybernetických hrozeb a poskytovat komplexní ochranu pro organizace všech velikostí.

Trendy v oblasti síťové bezpečnosti

Kybernetické hrozby se v posledních letech vyznačují rostoucí sofistikovaností a objemem útoků, přičemž bývá stále častěji využívána automatizace a pokročilé techniky sociálního

inženýrství. Podle zprávy společnosti FireEye (2023) je v současnosti více než 70 % kybernetických útoků prováděno automatizovanými nástroji, které umožňují skenování zranitelností a přizpůsobování metod útoků na základě aktuálních podmínek v cílové síti.

Jedním z klíčových trendů v oblasti síťové bezpečnosti je rostoucí důraz na síťovou viditelnost, která zahrnuje detailní sledování všech aspektů síťového provozu a schopnost detekovat subtilní anomálie, jež mohou signalizovat probíhající útok. Tradiční bezpečnostní metody, založené převážně na statických pravidlech a signaturách, se ukazují jako nedostatečné proti moderním hrozbám, jako jsou zero-day útoky, ransomwarové kampaně nebo APT. Tento vývoj vyžaduje nasazení pokročilých nástrojů, které dokáží pružně reagovat na neznámé typy útoků a adaptovat své detekční mechanismy na měnící se hrozby (ENISA, 2023).

Dalším významným trendem je integrace bezpečnostních řešení do jednotných platforem, které umožňují automatizovanou detekci a reakci na bezpečnostní incidenty v reálném čase. Síťová bezpečnost se stále častěji propojuje s forenzní analýzou, správou zranitelností a preventivní detekcí hrozeb, což zajišťuje efektivnější řízení rizik a minimalizaci dopadů kybernetických útoků. Přístup založený na propojení více bezpečnostních komponent a jejich vzájemné komunikaci umožňuje komplexnější a rychlejší reakce na bezpečnostní incidenty (Gartner, 2023).

Vliv AI a strojového učení na detekci anomálií

Umělá inteligence (AI) a strojové učení se v současnosti řadí mezi nejvýznamnější technologie, které mění přístup k detekci kybernetických hrozeb. Tyto pokročilé metody umožňují automatickou detekci anomálií a efektivnější analýzu síťového provozu, než jaké nabízí tradiční metody založené výhradně na signaturách. V systému Flowmon se strojové učení již uplatňuje prostřednictvím modulu ADS, který umožňuje identifikaci neobvyklých vzorců chování a detekci hrozeb, jež by jinými nástroji nebyly zachyceny (Flowmon, 2023).

V oblasti síťové bezpečnosti bývá využití umělé inteligence zaměřeno zejména na schopnost analyzovat velké objemy síťových dat a identifikovat odchylky od běžného provozu. Tento přístup umožňuje generovat prediktivní modely hrozeb, což významně zvyšuje schopnost detekce i v prostředích s vysokou variabilitou síťové komunikace. Strojové učení umožňuje automatizované rozpoznávání neznámých útoků, adaptaci na nové typy hrozeb a významné snížení míry falešně pozitivních detekcí. Tyto výhody jsou zásadní zejména při nasazování

bezpečnostních řešení v rozsáhlých podnikových sítích, kde se denně přenášejí obrovské objemy dat (McGregor, 2021).

Budoucí vývoj systému Flowmon bude pravděpodobně směřován k hlubší integraci AI do bezpečnostních procesů, což má umožnit ještě vyšší efektivitu při detekci pokročilých útoků v reálném čase. Předpokládá se, že v následujících letech dojde k zavedení pokročilejších modelů strojového učení, které budou schopny detekovat anomálie nejen na úrovni jednotlivých organizací, ale i v globálním měřítku. Tento přístup by měl umožnit prediktivní detekci útoků v rámci celé komunity uživatelů Flowmonu, což výrazně zvýší bezpečnostní standardy i ve složitých prostředích s různorodou infrastrukturou (Progress, 2021).

Možný vývoj Flowmonu v následujících letech

Budoucí vývoj systému Flowmon bude pravděpodobně směřovat k automatizovanému řízení bezpečnostních událostí a hlubší integraci s dalšími nástroji kybernetické ochrany. Jedním z klíčových směrů vývoje bude zřejmě posílení orchestrace bezpečnostních procesů, což umožní automatizovanou reakci na detekované hrozby bez nutnosti manuálního zásahu správce sítě. Takové vylepšení má potenciál výrazně snížit reakční dobu při výskytu bezpečnostních incidentů a zvýšit celkovou efektivitu ochrany síťového provozu (Flowmon, 2023).

Dále se předpokládá, že bude docházet k rozvoji v oblasti pokročilé analytiky pro prediktivní bezpečnost, což zahrnuje využívání historických dat o síťovém provozu k předpovídání potenciálních bezpečnostních incidentů ještě před jejich samotným výskytem. Tento přístup, označovaný jako proaktivní bezpečnostní analýza, již bývá implementován v některých pokročilých bezpečnostních systémech, avšak jeho aplikace v oblasti síťového monitorování se nachází stále v rané fázi vývoje (Cisco, 2023).

Vzhledem k rostoucí poptávce po cloudových bezpečnostních řešeních bude pravděpodobně vývoj Flowmonu směřován i ke zvýšení schopnosti nasazení v hybridních a multi-cloudových prostředích. Tento trend je patrný zejména v korporátním segmentu, kde bývá nutné sledovat provoz nejen v rámci interní infrastruktury, ale také v cloudových službách typu AWS, Azure nebo Google Cloud. Úspěšná implementace tohoto přístupu umožní širší využití Flowmonu v moderních IT prostředích, která jsou založena na decentralizované infrastruktuře (ENISA, 2023).

Dalším významným směrem rozvoje bude pravděpodobně větší propojení Flowmonu s konceptem Zero Trust architektury, která se stále častěji prosazuje jako standardní model

pro řízení bezpečnosti v podnikových sítích. Tento přístup vyžaduje neustálé monitorování a ověřování každého uživatele a zařízení v síti, což Flowmon umožňuje díky svým pokročilým možnostem analýzy síťového provozu. Integrace těchto principů do Flowmonu by mohla výrazně zvýšit jeho schopnost poskytovat komplexní ochranu před hrozbami na všech úrovních infrastruktury (Gartner, 2023).

3.4 Regulace a legislativní požadavky na monitorování sítí

Směrnice NIS2, která vstoupila v platnost v roce 2023, představuje významný krok v oblasti kybernetické bezpečnosti na úrovni Evropské unie. Hlavním cílem této směrnice je zvýšit odolnost klíčových infrastruktur vůči kybernetickým hrozbám prostřednictvím povinného monitorování síťového provozu a zavádění detekčních mechanismů pro včasné odhalování potenciálních útoků. Flowmon je v tomto ohledu vnímán jako nástroj, který umožňuje plnit požadavky směrnice NIS2, protože poskytuje schopnost monitorovat síťový provoz v reálném čase, analyzovat bezpečnostní události a reagovat na detekované hrozby prostřednictvím automatizovaných procesů (ENISA, 2023).

GDPR a ochrana síťových dat

Obecné nařízení o ochraně osobních údajů (GDPR) klade důraz na bezpečné zpracování síťových dat, zejména v případech, kdy obsahují osobně identifikovatelné informace. Flowmon umožňuje nasazení nástrojů pro anonymizaci a šifrování síťových toků, což zajišťuje, že zpracovávaná data jsou chráněna před neoprávněným přístupem a v souladu s platnými právními předpisy. Tímto způsobem bývá dosaženo nejen splnění požadavků GDPR, ale také zvýšení celkové úrovně zabezpečení síťové komunikace (Cisco, 2023).

4 SHRNUÍ TEORETICKÉ ČÁSTI

V teoretické části této práce byla podrobně analyzována problematika kybernetické bezpečnosti, monitorování síťového provozu a využití platformy Flowmon jako aktivního bezpečnostního řešení. S rostoucím množstvím kybernetických hrozeb a stále sofistikovanějšími metodami útoků je efektivní monitorování síťového provozu klíčovým prvkem obrany proti narušení bezpečnosti. Tradiční přístupy, jako jsou firewally a IDS/IPS systémy, již nejsou samy o sobě dostatečné, protože nedokáží odhalit pokročilé útoky, jako jsou zero-day hrozby, pokusy o laterální pohyb útočníků v síti a útoky využívající šifrovaný provoz.

Flowmon v tomto kontextu představuje moderní bezpečnostní platformu, která kombinuje pokročilou analýzu síťových toků, detekci anomálií a automatizovanou reakci na bezpečnostní incidenty. Na rozdíl od tradičních nástrojů se nespolehá pouze na signatury a pravidla, ale využívá behaviorální analýzu a strojové učení, což umožňuje detekovat i dosud neznámé hrozby. Flowmon tak poskytuje komplexní přehled o síťovém provozu a umožňuje identifikovat a minimalizovat bezpečnostní rizika v reálném čase (Flowmon, 2023).

V rámci teoretické části byla také popsána architektura Flowmonu, která zahrnuje senzory pro sběr síťových toků, kolektory pro analýzu dat a centrální řídicí konzoli, která poskytuje přehled o provozu v síti a umožňuje správu bezpečnostních incidentů. Flowmon nabízí několik specializovaných modulů, mezi které patří Flowmon ADS pro detekci anomálií, Flowmon DDoS Defender pro ochranu před distribuovanými útoky a Flowmon Monitoring Center pro vizualizaci a správu síťového provozu (Progress, 2021).

Kapitola o srovnání s jinými bezpečnostními řešeními ukázala, že Flowmon nabízí významné výhody oproti tradičním IDS/IPS systémům a dalším monitorovacím platformám, jako jsou Cisco Stealthwatch nebo Darktrace. Zatímco IDS/IPS systémy pracují primárně na základě signatur známých hrozeb, Flowmon využívá behaviorální analýzu síťového provozu, čímž dokáže detekovat i neznámé útoky, které signaturami nejsou pokryty. V porovnání s řešeními jako Cisco Stealthwatch má Flowmon větší flexibilitu nasazení, protože podporuje různé síťové technologie, zatímco Cisco Stealthwatch je úzce vázán na síťovou infrastrukturu Cisco. Oproti Darktrace, který využívá hluboké neuronové sítě pro analýzu provozu, nabízí Flowmon vyváženější poměr mezi výkonem a provozními náklady, což jej činí vhodným i pro organizace s omezenými bezpečnostními rozpočty (Cisco, 2023).

Důležitým aspektem Flowmonu je také jeho schopnost integrace s dalšími bezpečnostními nástroji, jako jsou firewally, SIEM systémy a systémy pro správu zranitelností. Díky podpoře automatizovaných reakcí umožňuje Flowmon rychlou mitigaci bezpečnostních incidentů, například automatické blokování útočníků na firewallu, generování výstrah nebo spolupráci s DDoS ochrannými službami. Tento přístup minimalizuje reakční dobu na kybernetické hrozby a zvyšuje celkovou odolnost organizace vůči útokům (Progress, 2021).

V rámci budoucího vývoje se očekává, že Flowmon bude stále více využívat umělou inteligenci a strojové učení k automatizované detekci a prevenci kybernetických útoků. S rostoucím důrazem na Zero Trust bezpečnostní modely a monitorování hybridních cloudových infrastruktur bude Flowmon pravděpodobně rozšiřovat své schopnosti o větší podporu cloudových prostředí a pokročilou prediktivní analýzu síťového provozu. Vzhledem k tomu, že organizace čelí stále sofistikovanějším kybernetickým hrozbám, lze očekávat, že technologie automatizované detekce hrozeb a autonomního řízení bezpečnostních politik se stane nezbytnou součástí ochrany podnikových sítí (ENISA, 2023).

Flowmon tak představuje moderní a adaptabilní řešení, které se neomezuje pouze na monitorování provozu, ale aktivně přispívá k ochraně podnikových sítí. Díky své modularitě, možnosti integrace s dalšími bezpečnostními systémy a využití pokročilých analytických metod poskytuje komplexní přístup k síťové bezpečnosti, což jej činí efektivním nástrojem pro organizace všech velikostí.

II. PRAKTICKÁ ČÁST

5 ANALÝZA FUNKCIONALITY NÁSTROJE FLOWMON V REÁLNÉM PROSTŘEDÍ

Testování nástroje Flowmon bylo provedeno v prostředí univerzitní sítě Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně, konkrétně v areálu v Uherském Hradišti. Tato fakulta je součástí jedné z největších veřejných vysokých škol v České republice a disponuje vlastní počítačovou sítí, která slouží jak pro výukové, tak výzkumné účely. Infrastruktura této sítě zahrnuje také podporu administrativních činností, přičemž provoz je využíván desítkami zaměstnanců a stovkami studentů v každodenním provozu.

Síť je navržena jako samostatný segment univerzitní páteřní sítě a je spravována interními správci IT. Architektura je tvořena kombinací centrálně spravovaných serverů, koncových uživatelských zařízení a dalších specializovaných prvků, které jsou rozděleny do různých VLAN podle určení. Toto členění umožňuje segmentaci provozu na základě potřeb konkrétních uživatelů nebo služeb a zajišťuje lepší bezpečnostní i provozní správu.

Fyzická síťová infrastruktura se skládá z přepínačů druhé a třetí vrstvy (L2 a L3), směrovačů a bezdrátových přístupových bodů s podporou standardu IEEE 802.11ac. Tyto přístupové body zajišťují bezdrátové pokrytí v prostorách určených jak pro výuku, tak pro administrativní činnost. K síti je připojeno přibližně 300 zařízení, mezi něž patří osobní počítače, notebooky, tiskárny, síťová úložiště (NAS), univerzitní servery, přístupové body Wi-Fi a zařízení typu internet věcí (IoT).

Páteřní síť je tvořena hlavním L3 přepínačem, na který jsou připojeny další distribuční přepínače rozmístěné po jednotlivých budovách a serverovnách. Komunikace mezi těmito segmenty probíhá směrovaně a je řízena pomocí Access Control Lists (ACL), které zajišťují bezpečnost a oddělení jednotlivých VLAN.

Pro přístup k bezdrátové síti jsou využívány přístupové body podporující protokoly 802.11ac a 802.11n, které zajišťují kompatibilitu se širokou škálou zařízení. Bezdrátová síť zahrnuje také zabezpečený přístup pro studenty a zaměstnance pomocí WPA2-Enterprise s autentizací na bázi RADIUS serveru.

Síť byla navržena s důrazem na stabilitu, dostupnost a bezpečnost, přičemž jednotlivé segmenty jsou logicky odděleny pomocí VLAN. Toto členění slouží k minimalizaci rizik spojených s případným bezpečnostním incidentem v jednom segmentu a umožňuje efektivnější správu provozu.

V rámci této sítě probíhá jak vnitřní komunikace mezi servery a klienty, tak i komunikace s externím prostředím prostřednictvím připojení do internetu. Přístup do internetu je směřován přes centrální směrovače, které podporují export tokových dat pomocí protokolu NetFlow v9. Tyto toky jsou následně zpracovávány nástrojem Flowmon pro potřeby monitorování a analýzy provozu.

Univerzitní síť je považována za středně velkou síť s různorodým provozem, který zahrnuje jak běžnou uživatelskou komunikaci, tak specifické provozy spojené s výukovými a výzkumnými aktivitami. Nasazení Flowmonu v tomto prostředí umožnilo sledovat a analyzovat komunikaci na různých úrovních, od základní síťové vrstvy až po aplikační protokoly, což bylo klíčové pro další detekci anomálií a optimalizaci síťového provozu.

Pro účely monitorování síťového provozu a detekce anomálií v univerzitní síti Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně byl zvolen systém Flowmon, a to díky jeho kompatibilitě s protokoly NetFlow v9, IPFIX a sFlow, nízkým nárokům na hardware a možnosti nasazení jako virtuální appliance bez nutnosti zásahu do fyzické infrastruktury. Hlavními výhodami byly schopnost detekovat anomálie na základě tokových dat bez inspekce paketů, přítomnost modulu Flowmon ADS využívajícího heuristiku a strojové učení, a možnost integrace s dalšími bezpečnostními nástroji (např. SIEM systémy). Díky podpoře standardizovaných protokolů a akademickým licencím představoval Flowmon dostupné a flexibilní řešení, které umožnilo nejen detekci hrozeb, ale i optimalizaci provozu a dlouhodobé sledování síťových trendů. Nasazení v prostředí UTB proběhlo prostřednictvím dvou monitorovacích portů s přenosovou rychlostí 10 Gb/s, přičemž systém byl provozován v rámci virtualizační infrastruktury fakulty.

VLAN segmentace a logická architektura sítě

Pro efektivní správu a zabezpečení univerzitní sítě Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně byla implementována technologie VLAN (Virtual Local Area Network), která umožňuje rozdělit fyzickou infrastrukturu do několika logických segmentů. Cílem segmentace bylo oddělit různé typy provozu, zvýšit bezpečnost komunikace a usnadnit správu síťových zařízení.

Síťová infrastruktura je tvořena směrovači a přepínači druhé a třetí vrstvy (L2 a L3), které jsou rozmístěny v jednotlivých budovách a propojeny prostřednictvím pátečního přepínače umístěného v centrální serverovně. Tento hlavní přepínač funguje jako distribuční bod, který

zajišťuje směrování provozu mezi jednotlivými VLAN a propojení s externím prostředím (internetem).

V testovaném prostředí bylo identifikováno několik hlavních VLAN, které byly vytvořeny na základě funkčního rozdělení sítě:

VLAN 10 – Administrativa: Segment určený pro pracovní stanice administrativních zaměstnanců, servery s citlivými daty a zařízení vyžadující vyšší úroveň zabezpečení. Přístup do této VLAN je striktně řízen pomocí ACL, které zabraňují neoprávněnému přístupu z jiných segmentů.

VLAN 20 – Studenti: VLAN určená pro výukové účely a připojení studentských zařízení. Tato VLAN má přístup k vybraným službám, jako jsou e-learningové systémy a internet, avšak je omezená v přístupu ke kritickým serverům v rámci VLAN 10.

VLAN 30 – Bezdrátová síť (Wi-Fi): Segment vyhrazený pro přístupová zařízení podporující protokoly 802.11ac a 802.11n. Tato VLAN zahrnuje jak interní bezdrátovou síť pro studenty a zaměstnance (WPA2-Enterprise), tak i otevřenou síť pro hosty s omezeným přístupem.

VLAN 40 – Servery a úložiště: VLAN určená pro centrální servery, síťová úložiště (NAS) a kritické služby, které jsou nezbytné pro chod celé fakulty. Tento segment je oddělen od ostatních částí sítě a přístup je povolen pouze z určených VLAN.

VLAN 50 – IoT zařízení: Speciální VLAN vytvořená pro připojení síťových zařízení typu IoT, jako jsou tiskárny, kamery, klimatizační jednotky apod. Tento segment je izolován od ostatních částí sítě, což snižuje riziko potenciálního útoku na ostatní zařízení.

Komunikace mezi jednotlivými VLAN je možná pouze na základě předem definovaných pravidel, která jsou nastavena na L3 přepínači. Tyto pravidla zahrnují zejména ACL, které určují povolené směry komunikace, protokoly a porty. Například studenti ve VLAN 20 nemají přístup k serverům v VLAN 40, zatímco zařízení v administrativní VLAN 10 mohou využívat služby poskytované serverovou VLAN.

Všechny VLAN jsou spravovány centrálním směrovačem, který také provádí směrování mezi VLAN (Inter-VLAN Routing). Díky tomuto uspořádání je možné efektivně řídit provoz mezi různými částmi sítě a zároveň udržovat jejich izolaci tam, kde je to potřeba. Tím se zvyšuje jak bezpečnost, tak stabilita celé infrastruktury.

Pro zajištění bezdrátového připojení byla využita přístupová zařízení podporující protokoly 802.11ac a 802.11n, které poskytují dostatečnou kapacitu i při vyšší hustotě připojení. Přístupové body jsou spravovány centrálně, což umožňuje jednoduchou konfiguraci a monitoring.

Nasazený systém Flowmon využívá tuto segmentaci k tomu, aby mohl efektivně sledovat provoz mezi jednotlivými VLAN a identifikovat potenciální bezpečnostní incidenty. Toková data jsou shromažďována z více exportních bodů umístěných na úrovni L3 přepínače a následně analyzována pomocí nástroje Flowmon Collector. To umožňuje přesně určit, mezi kterými VLAN dochází ke zvýšenému provozu nebo neobvyklé aktivitě.

Technické nasazení systému

Nasazení nástroje Flowmon v prostředí univerzitní sítě Fakulty logistiky a krizového řízení Univerzity Tomáše Bati bylo realizováno jako softwarová virtuální appliance, která byla provozována ve virtualizačním prostředí fakulty. Tento přístup umožnil provoz systému bez nutnosti pořizování nového hardwaru a poskytl flexibilitu při nastavování a škálování monitorovací infrastruktury. Zvolená konfigurace nesla označení Flowmon Probe 2000 VA, která je vhodná pro středně velké sítě a umožňuje zpracování vysokého objemu tokových dat s dostatečnou přesností a rychlostí.

Pro účely testování byla appliance vybavena dvěma gigabajty operační paměti a provozována na dedikovaném jádru hostitelského systému. Nasazený software běžel na verzi Flowmon OS 12.04.03, která patřila mezi aktuální a stabilní verze s plnou podporou dostupných modulů, včetně Flowmon ADS a Monitoring Center.

Příjem tokových dat byl zajištěn prostřednictvím dvou monitorovacích portů označených jako eth2 a eth3, které byly nakonfigurovány na rychlost 10 000 Mb/s v plně duplexním režimu. Automatické vyjednávání linky bylo aktivní a standardní MTU (Maximum Transmission Unit) byla nastavena na 1500 bajtů. Zvolený přístup umožnil zachytávání veškerého provozu bez vzorkování (sampling rate: 0), což výrazně zvýšilo přesnost analýzy a schopnost detekce anomálií.

Toková data byla exportována z centrálního L3 přepínače a směrovače, které byly součástí univerzitní sítě. Přenos dat do Flowmonu probíhal pomocí protokolu NetFlow v9 a IPFIX, přičemž výstupy byly směrovány na IP adresu 10.32.26.65 a port User Datagram Protocol (UDP) 2055. Tento způsob přenosu umožnil zachytit komunikaci mezi jednotlivými VLAN i provoz směrovaný do externí sítě.

Protokol IPFIX byl zvolen jako hlavní zdroj dat z důvodu své flexibility a možnosti zasílat rozšířené informace o komunikaci. Byly využívány rozšířené záznamy zahrnující VLAN identifikátory, MAC adresy, Transmission Control Protocol (TCP) příznaky, L7 protokoly (DNS, HTTP, TLS fingerprinting JA3, Samba, VoIP, DHCP) a další aplikační metadata. Exportní šablony byly pravidelně obnovovány každých 4096 paketů nebo každých 600 sekund, což umožňovalo detailní sledování síťové aktivity.

Uložení tokových dat bylo realizováno v rámci modulu Flowmon Monitoring Center, který poskytoval přehledné rozhraní pro vizualizaci, filtrování a analýzu zachycených záznamů. Data byla ukládána s časovou granularitou umožňující zpětnou analýzu provozu až 183 dní zpětně, což bylo nastaveno jako výchozí hodnota pro retenci záznamů. Tento přístup poskytoval dostatečně dlouhé období pro zkoumání historických incidentů a detekci dlouhodobých trendů.

Z technického hlediska byla konfigurace systému provedena prostřednictvím webového rozhraní Flowmonu, které umožňovalo správu veškerých komponent, včetně nastavení monitorovacích portů, správy exportérů, nastavování citlivosti detekčních metod a správy výstrah. Veškerá komunikace s administrátorským rozhraním probíhala šifrovaně pomocí protokolu HyperText Transfer Protocol Secure (HTTPS), což zajišťovalo bezpečnost přístupu a minimalizovalo riziko neoprávněných zásahů.

Velkou výhodou bylo, že celý systém byl implementován bez nutnosti fyzických zásahů do existující infrastruktury. Instalace Flowmonu byla provedena jako pasivní monitoring prostřednictvím exportu tokových dat z již existujících zařízení, což minimalizovalo riziko výpadků nebo narušení provozu. Testované prostředí bylo zcela samostatné, což umožnilo provádět konfiguraci a změny bez dopadu na ostatní součásti univerzitní sítě.

Provoz systému byl rovněž monitorován pomocí systémových logů dostupných v rozhraní Flowmonu. Logy umožňovaly sledovat stav jednotlivých komponent, vytížení systému a potenciální problémy spojené se zpracováním tokových dat. Tato možnost se ukázala jako užitečná zejména při diagnostice problémů se synchronizací nebo při optimalizaci nastavení.

Nasazení Flowmonu v prostředí univerzitní sítě bylo úspěšné a umožnilo nejen monitorování síťového provozu v reálném čase, ale také dlouhodobé ukládání a analýzu dat. Tento přístup byl hodnocen jako efektivní a spolehlivý způsob, jak sledovat provoz univerzitní infrastruktury a identifikovat případné bezpečnostní incidenty.

Konfigurace monitorovacích portů

Konfigurace monitorovacích portů představovala klíčový krok při nasazení systému Flowmon v prostředí univerzitní sítě. Vzhledem k tomu, že systém Flowmon byl provozován jako softwarová virtuální appliance, bylo nutné správně nastavit rozhraní, která sloužila pro příjem tokových dat a jejich následnou analýzu. Monitorovací porty byly označeny jako eth2 a eth3 a byly nakonfigurovány tak, aby zajišťovaly nepřetržitý příjem a zpracování veškerého provozu, který byl exportován z páteřních síťových zařízení.

Rozhraní eth2 a eth3 byla provozována ve full-duplexním režimu s rychlostí 10 000 Mb/s, což odpovídalo moderním standardům pro páteřní síťová spojení. Automatické vyjednávání (autonegotiation) bylo aktivní a konfigurace umožňovala dynamické přizpůsobení linkových parametrů v případě změn na fyzické vrstvě. Hodnota MTU byla nastavena na 1500 bajtů, což je standardní velikost pro Ethernetová připojení a umožňuje zpracování běžného síťového provozu bez fragmentace.

Jedním z klíčových parametrů konfigurace bylo rozhodnutí nevyužívat vzorkování paketů (sampling rate: 0). Tento přístup zajistil, že všechny toky byly zachyceny bez redukce dat, což umožnilo provádět detailní analýzu komunikace a detekovat i jemné anomálie, které by při vzorkování nemusely být zaznamenány. Tento přístup však kladl vyšší nároky na výkon systému, což bylo v prostředí univerzitní sítě akceptovatelné vzhledem k velikosti sítě a objemu přenášených dat.

Pro přenos tokových dat byla použita kombinace protokolů NetFlow v9 a IPFIX, které byly exportovány z hlavního L3 přepínače a centrálního směrovače. Toky byly směrovány na IP adresu 10.32.26.65 prostřednictvím portu UDP 2055, což odpovídá standardní konfiguraci pro IPFIX přenosy. Monitorovací porty byly tedy nastavovány jako pasivní přijímače těchto dat, bez nutnosti zrcadlení provozu nebo konfigurace TAP zařízení.

Důležitým nastavením byla konfigurace aktivního a neaktivního timeoutu pro ukončování toků. Aktivní timeout byl nastaven na 300 sekund, zatímco neaktivní timeout činil 30 sekund. Tento mechanismus umožňoval pravidelné ukončování dlouhotrvajících spojení i těch, která se po určitou dobu neaktualizovala. Díky tomuto nastavení byl systém schopen pravidelně aktualizovat záznamy a poskytovat aktuální přehled o provozu.

Monitorovací porty byly rovněž nakonfigurovány tak, aby přijímaly rozšířené tokové záznamy, zahrnující informace o VLAN identifikátorech, MAC adresách, TCP příznacích, aplikačních protokolech a dalších rozšířených metadatech. Tento přístup umožňoval

provádět detailní analýzu provozu, například rozlišovat komunikaci v různých VLAN nebo sledovat aplikační provoz včetně protokolů jako DNS, HTTP, TLS, Samba, VoIP a DHCP. Zaznamenávání protokolů jako TLS fingerprinting JA3 bylo důležité zejména pro detekci šifrovaných spojení, která mohou představovat bezpečnostní riziko.

Výstupy z monitorovacích portů byly následně předávány do komponenty Flowmon Collector, která zajišťovala zpracování, ukládání a vizualizaci tokových dat. Konfigurace monitorovacích portů byla nastavena tak, aby minimalizovala riziko ztráty dat a maximalizovala přesnost detekce. Výběr metod, jako je zachytávání kompletních toků bez vzorkování a využívání rozšířených exportů, umožnil detailní sledování síťového provozu a poskytl dostatek informací pro následnou analýzu pomocí modulu Flowmon ADS.

Díky správné konfiguraci monitorovacích portů bylo možné provádět podrobnou analýzu komunikace mezi jednotlivými VLAN, identifikovat klíčové provozní uzly a sledovat případné bezpečnostní incidenty v reálném čase. Přesnost konfigurace byla klíčová pro úspěšné nasazení systému a umožnila využít plný potenciál nástroje Flowmon pro monitoring univerzitní sítě.

Ukládání a zpracování dat

Po konfiguraci monitorovacích portů a spuštění sběru tokových dat bylo dalším zásadním krokem nastavení jejich ukládání a následného zpracování. Data byla shromažďována a analyzována prostřednictvím komponenty Flowmon Collector, která byla nainstalována jako virtuální appliance v prostředí univerzitní sítě. Hlavním účelem této komponenty bylo zajištění stabilního a efektivního zpracování velkého objemu síťových toků a jejich ukládání do interní databáze pro další analýzu.

Toková data byla přijímána v pravidelných intervalech a ukládána s vysokou granularitou, což znamená, že každý zaznamenaný tok obsahoval detailní informace o komunikaci mezi jednotlivými zařízeními. Tyto záznamy zahrnovaly zdrojovou a cílovou IP adresu, zdrojový a cílový port, použitý protokol, objem přenesených dat, počet přenesených paketů, trvání komunikace, VLAN identifikátor, MAC adresu a případně i aplikaci identifikovanou pomocí NBAR2 klasifikace. Tento přístup umožnil podrobnou analýzu síťového provozu i bez nutnosti inspekce samotného obsahu paketů.

Systém byl konfigurován tak, aby toková data byla ukládána po dobu až 183 dní, což odpovídalo výchozímu nastavení retence dat v modulu Flowmon Monitoring Center. Tato dlouhá doba uchování umožňovala nejen detekci dlouhodobých trendů a anomálií, ale také

provádění retrospektivních analýz v případě, že byl zjištěn bezpečnostní incident. Výhoda tohoto přístupu spočívala v tom, že jakýkoli bezpečnostní nebo provozní problém mohl být zpětně prozkoumán na základě kompletního záznamu o komunikaci.

Ukládání dat probíhalo prostřednictvím proprietární databáze systému Flowmon, která byla optimalizována pro rychlé dotazování a filtrování velkých objemů tokových záznamů. Data bylo možné snadno prohledávat podle různých kritérií, jako jsou časové období, IP adresa, číslo portu, VLAN identifikátor nebo protokol. Tento způsob organizace dat poskytoval vysokou flexibilitu při analýze jak bezpečnostních hrozeb, tak provozních anomálií.

Kromě běžného provozního ukládání dat bylo důležité správně nastavit i mechanismus jejich rotace a archivace. Systém byl konfigurován tak, aby automaticky odstraňoval nejstarší záznamy po překročení stanovené doby uchování. Tento proces byl zajištěn bez nutnosti zásahu administrátora a byl navržen tak, aby nedocházelo k přetížení úložiště ani ke ztrátě důležitých informací.

Pro zajištění vysoké dostupnosti a efektivity systému bylo využito funkce aktivního a neaktivního timeoutu pro ukončování toků. Aktivní timeout byl nastaven na 300 sekund, což znamená, že pokud komunikace probíhala kontinuálně déle než pět minut, došlo k jejímu ukončení a vytvoření nového záznamu. Neaktivní timeout byl naopak nastaven na 30 sekund, což zajišťovalo, že spojení, která byla ukončena nebo se po určitou dobu neaktualizovala, byla správně zaznamenána a uzavřena.

Data uložená v systému Flowmon Collector byla následně zpracovávána nejen pro účely běžného monitorování, ale také pro detekci anomálií prostřednictvím modulu Flowmon ADS. Tím bylo umožněno identifikovat neobvyklé vzorce chování v síťovém provozu, například pokusy o skenování portů, neoprávněný přístup nebo nestandardní objem přenášených dat. Tento analytický přístup poskytoval jak základní přehledy o síťovém provozu, tak i hloubkovou analýzu pro účely bezpečnostního dohledu.

Díky použití systému Flowmon bylo možné monitorovat a ukládat toková data v reálném čase i retrospektivně. Data byla nejen ukládána, ale také strukturována tak, aby umožnila rychlé dotazování a generování přehledů pro různé účely. Tento přístup zvyšoval efektivitu provozu a umožňoval provádět detailní analýzy v případě potřeby.

Bezpečnostní a provozní poznatky

Implementace systému Flowmon v univerzitní síti poskytla cenné poznatky nejen o bezpečnostních aspektech provozu, ale také o jeho celkové stabilitě, výkonnosti a zatížení. V průběhu testování bylo možné identifikovat řadu situací, které by jinak mohly zůstat nepovšimnuty, a to zejména díky pokročilým analytickým funkcím dostupným prostřednictvím modulů Flowmon Monitoring Center a Flowmon ADS.

Jedním z nejvýznamnějších přínosů bylo detekování neautorizovaného přístupu a nestandardního chování ve vybraných VLAN. V rámci testování bylo opakovaně zjištěno, že zařízení ve studentské VLAN generují komunikaci, která neodpovídá běžnému provozu akademické sítě. Pomocí modulu Monitoring Center bylo zaznamenáno, že v nočních hodinách dochází k navazování šifrovaných spojení přes protokol HTTPS (TCP/443) směrem na neznámé IP adresy mimo univerzitní síť, což bylo považováno za potenciálně rizikové. Výstupy z Monitoring Center byly následně předány modulu Flowmon ADS, kde byly detekce korelovány s metodami UPLOAD a BLACKLIST. Na základě tohoto vyhodnocení bylo potvrzeno, že několik z těchto IP adres figurovalo na blacklistu, což nasvědčovalo možné škodlivé komunikaci.

Dalším zásadním zjištěním bylo, že univerzitní síť vykazuje vysoký objem broadcast provozu v určitých časových intervalech, zejména během výuky a přístupu studentů k e-learningovým platformám. Tento problém se projevil především v segmentu Wi-Fi sítě, kde docházelo k opakovaným ARP (Protokol pro zjištění MAC adresy) a DHCP požadavkům z různých zařízení. Z přehledů protokolů bylo patrné, že broadcastové bouře jsou generovány chybně nakonfigurovanými zařízeními nebo neefektivním routováním v rámci VLAN. Tento poznatek byl důležitý nejen pro zvýšení bezpečnosti, ale i pro optimalizaci výkonu sítě.

Modul Flowmon ADS rovněž poskytl důležité informace o podezřelé aktivitě související se skenováním portů a pokusy o přihlášení na univerzitní servery. Detekční metoda BruteForce byla schopna identifikovat opakované pokusy o přihlášení na specifické služby přes protokol Secure Shell (SSH) a Remote Desktop Protocol (RDP). Veškeré tyto incidenty byly označeny jako potenciálně nebezpečné a byly vyhodnoceny z hlediska jejich četnosti a původu. Ukázalo se, že některé pokusy pocházely z IP adres v rámci univerzitní sítě, což nasvědčovalo možnému zneužití zařízení připojených do Wi-Fi VLAN.

Z provozního hlediska bylo pozorováno, že univerzitní síť vykazuje nejvyšší zátěž během pracovních dnů mezi 8:00 a 13:00, což odpovídá běžnému rozvrhu výuky a pracovním aktivitám. Naopak v odpoledních a večerních hodinách byl provoz výrazně nižší, což umožňovalo provádět nezbytné údržby a aktualizace bez zásadního omezení uživatelského komfortu. Tento poznatek byl využit při plánování pravidelných záloh serverů a síťových prvků.

Z bezpečnostního hlediska se ukázalo, že modul Flowmon ADS poskytuje efektivní nástroj pro detekci anomálií, které by mohly být přehlédnuty standardními bezpečnostními opatřeními. Díky kombinaci metod behaviorální analýzy a pravidelných aktualizací blacklistů bylo možné rychle identifikovat komunikaci s potenciálně nebezpečnými zdroji, neoprávněné pokusy o přístup a neobvyklé přenosy velkých objemů dat.

Při analýze bylo rovněž zjištěno, že některé části sítě vykazují zvýšenou míru retransmisí TCP paketů, což naznačuje možné problémy na fyzické vrstvě, například rušení na Wi-Fi nebo nevhodnou konfiguraci síťových prvků. Tento jev byl zaznamenán především v prostředí bezdrátové sítě, kde byla hustota zařízení nejvyšší. Získané poznatky vedly k úpravě konfigurace přístupových bodů a optimalizaci jejich rozmístění, čímž bylo dosaženo zlepšení kvality přenosů.

Výsledky získané pomocí systému Flowmon nejen zvýšily úroveň bezpečnosti univerzitní sítě, ale také přispěly k její celkové optimalizaci a efektivnímu provozu. Modul ADS umožnil rychlé a přesné identifikování bezpečnostních incidentů a jejich vyhodnocení v kontextu běžného provozu. Tento přístup poskytl komplexní pohled na provozní stav infrastruktury a umožnil provést nezbytné změny v konfiguraci sítě, které vedly ke zvýšení její stability a odolnosti vůči vnějším i vnitřním hrozbám.

Role administrátora a přínos systému

Správa systému Flowmon v univerzitním prostředí byla zajišťována prostřednictvím webového rozhraní, které poskytovalo centrální přístup ke všem funkcím systému, včetně monitoringu, konfigurace, detekce hrozeb a reportování. Rozhraní bylo dostupné přes zabezpečený protokol HTTPS, což zajistilo bezpečnou komunikaci mezi administrátorem a serverem. Každý přihlášený uživatel musel být autentizován pomocí uživatelského jména a hesla, přičemž bylo možné přidělovat různá přístupová práva na základě role uživatele.

Jedním z hlavních úkolů administrátora bylo nastavení a správa detekčních metod v rámci modulu Flowmon ADS. Tento modul umožňuje konfigurovat různé detekční mechanismy,

jako jsou BruteForce, DNSAnomaly, UPLOAD nebo BLACKLIST, přičemž každý z nich se zaměřuje na specifický typ hrozby. Administrátor měl možnost upravovat citlivost těchto metod, definovat nové pravidla nebo měnit stávající, což bylo klíčové zejména při zvyšování přesnosti detekcí a snižování falešně pozitivních výsledků.

Rozhraní Flowmon bylo navrženo tak, aby poskytovalo rychlý přístup k nejdůležitějším statistikám a incidentům. Na hlavní obrazovce byly zobrazeny přehledy Top Hosts, Top protocols, Top Conversations a Top VLANs, což umožňovalo rychle identifikovat nejvytíženější zařízení, protokoly a komunikační relace v rámci sítě. Administrátor mohl pomocí filtrů okamžitě vyhledávat konkrétní zařízení nebo sledovat vývoj určitého typu provozu v čase.

Přínos systému se ukázal především při analýze bezpečnostních incidentů a jejich následné dokumentaci. Každý incident detekovaný modulem ADS byl zaznamenán s časovým údajem, popisem hrozby a doporučením dalšího postupu. Administrátor měl možnost incident potvrdit, označit jako falešně pozitivní nebo jej zařadit k dalšímu sledování. Všechny tyto akce byly evidovány a mohly být následně použity při vyhodnocování účinnosti systému nebo při vytváření pravidelných reportů.

Zásadní výhodou systému Flowmon bylo propojení s dalšími bezpečnostními nástroji, například firewally nebo SIEM systémy. Díky standardizovanému API bylo možné exportovat detekované incidenty do externích systémů nebo naopak importovat data o známých hrozbách. Tato schopnost zajišťovala komplexní přístup k bezpečnostnímu monitoringu a umožňovala reagovat na incidenty rychleji a efektivněji.

Administrátor měl rovněž přístup k možnostem automatizovaného reportování a zasílání upozornění. Flowmon umožňoval generování pravidelných reportů, které byly odesílány e-mailem na zadané adresy, případně bylo možné vytvářet automatizované notifikace na základě předem definovaných pravidel. Tyto funkce se osvědčily zejména při dlouhodobém sledování provozu a vyhodnocování trendů.

V rámci každodenní správy systému byla klíčová také možnost exportovat data pro externí analýzu nebo archivaci. Administrátor mohl z rozhraní Flowmon Monitoring Center exportovat přehledy ve formátu CSV, JSON nebo PDF, což umožňovalo jejich následné zpracování v dalších analytických nástrojích, případně jejich prezentaci vedení univerzity.

Kromě technických přínosů přinesl systém Flowmon i výrazné zlepšení provozní efektivity. Díky možnosti rychlého vyhodnocení bezpečnostních incidentů a jejich dokumentace bylo

možné lépe plánovat reakční opatření, optimalizovat konfiguraci sítě a předcházet potenciálním hrozbám. Administrátorům systém poskytl prostředí, které je nejen snadno ovladatelné, ale i přehledné a flexibilní.

Díky těmto vlastnostem se Flowmon stal nezbytným nástrojem pro správu univerzitní sítě, který umožnil nejen sledovat provoz a detekovat hrozby, ale také optimalizovat infrastrukturu a plánovat její rozvoj na základě reálných statistik a analytických výstupů. Tento přístup přispěl ke zvýšení stability a bezpečnosti celé sítě, což je v prostředí vysoké školy s rozsáhlou infrastrukturou a širokým spektrem uživatelů zásadní.

5.1 Flowmon Monitoring Center

Modul Flowmon Monitoring Center (FMC) představuje centrální nástroj pro vizualizaci, analýzu a správu síťového provozu v rámci systému Flowmon. Tento modul umožňuje administrátorům přehledně sledovat komunikaci mezi jednotlivými zařízeními, identifikovat provozní vzorce a anomálie, a v reálném čase reagovat na bezpečnostní incidenty. Monitoring Center funguje jako nadstavba nad kolektorem tokových dat, která poskytuje přístup k aktuálním i historickým informacím o provozu prostřednictvím intuitivního webového rozhraní.

V testovaném prostředí univerzitní sítě Fakulty krizového řízení a logistiky Univerzity Tomáše Bati bylo Flowmon Monitoring Center využíváno jako hlavní nástroj pro sledování síťového provozu ve všech VLAN a pro identifikaci případných problémů či bezpečnostních rizik. Data byla do FMC přiváděna z kolektoru prostřednictvím protokolů NetFlow v9 a IPFIX, což umožnilo detailní analýzu síťových toků bez nutnosti zpracovávat jednotlivé pakety. Tento přístup byl zvolen s ohledem na efektivitu systému a schopnost pracovat s velkým objemem dat bez výrazného zatížení infrastruktury.

Rozhraní modulu FMC bylo navrženo tak, aby poskytovalo přehledné a uživatelsky přívětivé prostředí, které je snadno použitelné i pro méně zkušené administrátory. Na úvodní obrazovce se nacházely souhrnné přehledy provozu, které byly přizpůsobitelné dle potřeb administrátora. Bylo možné sledovat komunikaci v reálném čase, analyzovat historické trendy nebo vytvářet automatizované reporty, které byly zasílány na e-mail nebo exportovány do různých formátů.

Monitoring Center umožňovalo administrátorům nastavit různé přehledy a filtry, díky čemuž bylo možné zobrazit například:

- Top Hosts – zařízení s největším objemem přenesených dat.
- Top Conversations – nejfrekventovanější komunikační relace mezi zařízeními.
- Top Protocols – nejčastěji používané protokoly (např. HTTPS, DNS, SMB).
- Top VLANs – přehled zátěže jednotlivých segmentů sítě.
- Top Applications – sledování komunikace na aplikační vrstvě.

Jednou z nejvýznamnějších funkcí FMC je schopnost sledovat síťové toky na základě časových řad. Administrátoři mohou detailně zkoumat provoz v určitých časových intervalech, porovnávat jednotlivé dny nebo týdny a odhalovat odchylky od běžného chování. Tato schopnost se ukázala jako klíčová při identifikaci provozních problémů, jako jsou přetížení sítě, neoprávněné přístupy nebo anomálie způsobené nesprávnou konfigurací zařízení.

V testovaném prostředí bylo Flowmon Monitoring Center také využíváno pro tvorbu pravidelných reportů, které byly generovány automaticky na základě předem definovaných šablon. Tyto reporty obsahovaly například přehledy nejvytíženějších zařízení, objemy přenesených dat, seznam nejčastěji využívaných protokolů a identifikaci potenciálně rizikových komunikací.

Důležitým aspektem modulu Monitoring Center byla rovněž jeho schopnost spolupráce s dalšími komponentami systému Flowmon, především s modulem Flowmon ADS. Výsledky analýzy síťového provozu mohly být přímo předávány ADS k dalšímu vyhodnocení a korelaci s detekčními pravidly.

Celkově lze říci, že Flowmon Monitoring Center v univerzitní síti poskytovalo komplexní přehled o provozu a umožňovalo efektivní správu infrastruktury. Administrátoři mohli rychle reagovat na změny v provozu, identifikovat problematické oblasti a přijímat vhodná opatření k zajištění bezpečnosti a stability sítě.

Analýza síťového provozu

V rámci modulu Flowmon Monitoring Center byla provedena analýza síťového provozu na základě tokových dat, která byla exportována ze síťových zařízení prostřednictvím protokolu NetFlow v9. Tento modul poskytuje přehledné a detailní informace o síťové komunikaci mezi jednotlivými uzly, což umožňuje rychle identifikovat potenciální problémy, detekovat bezpečnostní hrozby a optimalizovat provozní výkon sítě.

Prvním krokem analýzy bylo sledování nejvytíženějších zařízení v síti prostřednictvím přehledu Top Hosts. Tento přehled poskytuje informaci o IP adresách, které generují největší objem dat, a umožňuje správci sítě sledovat jejich komunikaci v různých časových intervalech. Tabulka 1 ukazuje seznam nejaktivnějších zařízení v univerzitní síti, z nichž většina patří do VLAN administrativy nebo jsou součástí serverové infrastruktury. Tento přehled umožnil například identifikaci zařízení, které provádělo zálohování velkého objemu dat během pracovního dne, což způsobovalo dočasné přetížení sítě.

Tabulka 1: TOP Hosts

Pořadí	IP adresa	VLAN	Přenesená data (GB)	Počet toků
1	10.32.138.247	Administrativa	12,4	15 500
2	10.32.142.193	Studenti	9,8	13 200
3	10.96.1.51	Serverová infrastruktura	8,1	10 100
4	10.96.1.50	Serverová infrastruktura	6,7	8 900
5	10.32.140.5	WIFI Acces	5,3	8 200

(zdroj: vlastní)

Další důležitou metrikou bylo sledování Top Protocols, které poskytuje přehled o tom, jaké síťové protokoly dominují v provozu a jaký je jejich podíl na celkovém objemu přenesených dat. Jak je patrné z Tabulka 2, nejvíce komunikace probíhalo prostřednictvím protokolu HTTPS (TCP/443), což je v souladu s očekáváním vzhledem k běžnému využívání internetových služeb a zabezpečené komunikace. Významný podíl provozu také tvoří DNS (UDP/53) a SMB (TCP/445), který byl v rámci testování detekován jako možný bezpečnostní rizikový faktor kvůli neautorizovanému sdílení souborů mezi jednotlivými zařízeními.

Tabulka 2: Top Protocols

Pořadí	Protokol	Provoz (MB)
1	HTTPS (TCP/443)	1200
2	HTTP (TCP/80)	800
3	SMB (TCP/445)	600
4	Neznámé (TCP/55555)	300
5	DNS (UDP/53)	200

(zdroj: vlastní)

Pro detailnější analýzu byly využívány přehledy Top Conversations, které zobrazují komunikaci mezi konkrétními IP adresami a umožňují identifikovat nejčastější a nejintenzivnější relace v síti. Tabulka 3 demonstruje komunikace, což napomohlo při optimalizaci síťových pravidel a detekci nežádoucího přístupu mezi různými VLAN.

Tabulka 3: Top Conversations

Pořadí	Zdrojová IP	Cílová IP	Popis komunikace	Přenesená data (GB)
1	10.32.138.247	10.96.1.51	Zálohování dat mezi stanicí a serverem	6,8
2	10.96.1.50	10.32.138.247	Synchronizace administrativních dat	5,9
3	10.32.140.5	8.8.8.8	Přístup na DNS resolver Google	4,3
4	10.96.1.51	10.32.140.5	Přenos laboratorních souborů	4,0
5	10.32.142.193	10.0.0.1	Možná neautorizovaná VPN komunikace	3,7

(zdroj: vlastní)

Přehled Top VLANs umožňuje sledovat podíl provozu mezi jednotlivými logickými segmenty sítě. Tabulka 4 ukazuje, že největší objem provozu generují VLAN přidělené serverové infrastruktuře a bezdrátové síti pro studenty. Tento poznatek potvrdil předpoklad, že provoz ve studentské VLAN je často výrazně vyšší než v ostatních segmentech, což vedlo k úpravě nastavení prioritizace a šířky pásma.

Tabulka 4: Top VLANs

Pořadí	VLAN ID	Popis	Přenesená data (GB)	Počet zařízení
1	10	Serverová infrastruktura	85,2	25
2	20	Bezdrátová síť studenti	64,7	120
3	30	Administrativní síť	59,1	40
4	40	Laboratorní zařízení	42,3	35
5	50	Hostovská zařízení	33,8	60

(zdroj: vlastní)

Analýza dat byla prováděna v reálném čase i retrospektivně, přičemž Flowmon Monitoring Center umožňovalo porovnávat provozní vzory mezi různými časovými obdobími. Například srovnáním dat z období před začátkem semestru a během něj bylo možné identifikovat zvýšenou zátěž způsobenou připojováním velkého množství zařízení do bezdrátové sítě. Tento nástroj se ukázal být klíčovým při plánování kapacitní optimalizace infrastruktury a umožnil lépe rozvrhnout pravidelné údržby a aktualizace systémů.

Díky pokročilým analytickým schopnostem systému Flowmon bylo možné identifikovat nejen hlavní zdroje provozu a vytíženost jednotlivých protokolů, ale také lokalizovat potencionální bezpečnostní rizika, která by byla bez použití specializovaného nástroje velmi obtížně detekovatelná. Celkově lze tedy říci, že Flowmon Monitoring Center poskytl komplexní přehled o dění v univerzitní síti a umožnilo efektivní dohled nad její stabilitou a bezpečností.

Diagnostika provozních problémů

V rámci monitorování univerzitní sítě prostřednictvím Flowmon Monitoring Center byla průběžně prováděna diagnostika provozních problémů, které by mohly negativně ovlivnit výkon nebo dostupnost klíčových služeb. Systém Flowmon umožnil efektivní identifikaci provozních potíží prostřednictvím analýzy síťových toků, vizualizace provozu a sledování anomálních událostí. Diagnostika byla realizována jak pomocí pravidelných kontrol síťových přehledů, tak prostřednictvím předdefinovaných alarmů a notifikací, které byly v systému nastaveny.

Během provozu byly detekovány různé typy problémů, které zahrnovaly zejména zvýšenou latenci, nadměrné využívání šířky pásma a chyby způsobené přetížením zařízení. Z analýzy časových řad a provozních statistik bylo zjištěno, že ke zvýšené latenci docházelo zejména v dopoledních hodinách, kdy byla síť nejvíce zatížena probíhající výukou a synchronizací dat mezi serverovými úložišti a koncovými zařízeními. Typickým příkladem byla situace, kdy velký počet zařízení připojených přes bezdrátovou síť (protokol 802.11ac) přistupoval ke stejným serverům ve VLAN určené pro učebny. Toto chování způsobovalo prodloužení doby odezvy a snížení kvality služeb poskytovaných prostřednictvím univerzitní sítě.

Dalším diagnostikovaným problémem bylo nadměrné využívání šířky pásma některými zařízeními, které generovaly velké objemy dat například při synchronizaci se vzdálenými úložišti nebo při stahování obsahu z internetu. Flowmon Monitoring Center umožnilo rychlou identifikaci těchto zařízení pomocí přehledů Top Hosts a Top Conversations, kde byly zobrazeny IP adresy generující největší provoz v rámci daného časového období. Tento typ analýzy byl klíčový pro odhalení nesprávně nakonfigurovaných zařízení nebo neautorizovaných činností, které mohly vést ke snížení výkonu sítě.

Během testování byly také zaznamenány případy broadcastových bouří způsobených nesprávnou konfigurací přepínačů v některých VLAN. K těmto incidentům docházelo zejména při propojení zařízení bez odpovídající konfigurace Spanning Tree Protocol (STP), což vedlo k cyklickému přenosu paketů a zahlcení síťového segmentu. Pomocí Flowmon Monitoring Center bylo možné detekovat zvýšený objem ARP a DHCP provozu, který nesouvisel s běžnou komunikací. Analýza těchto událostí umožnila rychlé nasazení protipatření a optimalizaci konfigurace síťových prvků.

Diagnostika provozních problémů rovněž zahrnovala sledování chybovosti spojení, které bylo zjišťováno pomocí analýzy retransmisí TCP paketů a neuzavřených spojení. Tyto jevy

byly často způsobeny nekvalitním bezdrátovým připojením, zejména v oblastech s vysokou hustotou připojených zařízení. Pomocí Flowmon Monitoring Center bylo možné přesně identifikovat postižené oblasti a navrhnout opatření k optimalizaci pokrytí nebo změně nastavení bezdrátových přístupových bodů.

Z provedené diagnostiky vyplynulo, že Flowmon Monitoring Center je efektivním nástrojem pro detekci nejen bezpečnostních incidentů, ale i běžných provozních problémů, které mohou negativně ovlivnit kvalitu síťových služeb. Možnost průběžné analýzy provozu, zpětného vyhledávání anomálních událostí a porovnávání historických dat umožňuje administrátorům identifikovat příčiny problémů rychleji a přesněji než při použití klasických metod sledování sítě.

Exporty, reporty a notifikace

Modul Flowmon Monitoring Center hraje zásadní roli při správě a dohledu nad síťovým provozem, a to především díky rozsáhlým možnostem exportu dat, tvorby pravidelných reportů a konfigurace notifikačních systémů. Tyto nástroje umožňují síťovým administrátorům získávat aktuální a historická data o síťové komunikaci, čímž přispívají k efektivnímu řízení síťového prostředí i zajištění bezpečnosti.

Export dat je v rámci systému často využíván pro další analýzu nebo archivaci, přičemž nejčastěji používanými formáty jsou CSV a JSON, které zajišťují širokou kompatibilitu s dalšími analytickými nástroji. Tato exportovaná data se následně využívají například při srovnávací analýze provozních trendů nebo při zpětném hodnocení bezpečnostních incidentů.

Generování reportů představuje další klíčovou funkcionalitu, díky níž mohou správci automaticky nebo manuálně vytvářet výstupy o síťovém chování. Reporty byly ve zkoumaném prostředí nejčastěji vytvářeny ve formátu PDF – vhodném pro prezentaci vedení – a CSV – využívaném při technické analýze. Šablony reportů byly předdefinovány tak, aby obsahovaly metriky jako počet toků, využití protokolů, počet aktivních IP adres nebo výskyt anomálií, a mohly být generovány denně, týdně nebo měsíčně dle potřeby.

Velmi přínosnou funkcí byla také konfigurace notifikací, které slouží jako rychlý mechanismus pro upozornění na události, jež vybočují z běžného provozu. Tyto notifikace byly doručovány primárně prostřednictvím e-mailu a Syslog zpráv do dalších systémů. Využívaly byly především při detekci pokusů o neautorizovaný přístup, zjištění komunikace s nežádoucími IP adresami, nebo při překročení definovaných prahových hodnot síťového

provozu. Díky nim bylo možné na vzniklé incidenty reagovat rychle a efektivně, a tím minimalizovat možné dopady na provoz univerzitní sítě. Tabulka 5 poukazuje na shrnutí těchto funkcí.

Tabulka 5: Funkce Flowmon Monitoring Center

Oblast funkce	Popis využití	Výstup/reakce
Export dat	Export přehledu (Top Hosts, Protocols) do CSV/JSON	Ruční/ plánovaný export na uložistiště
Generování reportů	Periodické měsíční/týdenní na základě šablon (aktivita serverů, VLAN provoz)	PDF/CSV, automatické odesílání e-mailem
Notifikace	Upozornění na překročení objemu dat, přístup z neznámých IP, provoz mimo pracovní dobu	E-mail, Syslog zpráva, případná eskalace
Integrace	Propojení s logovacím systémem, SIEM platformami	Možnost napojení na další bezpečnostní nástroje
Reálné příklady	Upozornění na noční přístupy na univerzitní servery	Okamžité varování správce

(zdroj: vlastní)

Přínosy Monitoring Center pro správu sítě

V rámci nasazení Flowmon Monitoring Center byly identifikovány konkrétní přínosy, které zásadně zefektivnily správu univerzitní sítě. Největší výhodou se ukázala být možnost okamžité vizualizace síťového provozu a rychlé detekce odchylek, které by bez pokročilého monitoringu zůstaly skryté.

V přehledu Top Hosts bylo například možné v několika případech okamžitě odhalit zařízení, která mimo pracovní dobu generovala neobvykle vysoký datový provoz – typicky šlo o přenosy větší než 10 GB za hodinu, a to z Wi-Fi segmentu. U těchto stanic byla následně prověřena konfigurace a logy přístupových bodů, přičemž u dvou z nich se potvrdila přítomnost aktivního synchronizačního klienta s cloudovým úložištěm mimo univerzitní doménu.

V jiné situaci přehled Top Conversations odhalil trvale probíhající spojení mezi učebnovou stanicí a serverem mimo fakultní síť. Komunikace běžela na portu TCP/443 a její objem za víkend přesáhl 30 GB. Po analýze bylo zjištěno, že se jedná o vzdálený přístup skrze TeamViewer, který nebyl správcem schválen. Aktivita byla zaznamenána a spojení zablokováno.

Díky retrospektivnímu přístupu k datům bylo možné porovnat síťový provoz během výukového období a zkouškového týdne. Byl potvrzen více než dvojnásobný nárůst DNS dotazů a výrazné zatížení VLAN segmentu knihovních stanic, což vedlo k rozhodnutí optimalizovat trasování těchto služeb.

Dále byly přes FMC zachyceny případy retransmisí TCP spojení, jejichž četnost se výrazně zvyšovala v dopoledních špičkách v laboratořích. To ukázalo na lokální problém s Wi-Fi přístupovými body, který byl později potvrzen výměnou zařízení a konfigurací roamingu.

Funkce notifikací byla využívána zejména při detekci provozu na vybraných portech v nočních hodinách. Díky těmto alertům bylo možné zaznamenat pokusy o přístup k univerzitním serverům mimo povolený rámec a tato aktivita byla dále zanesena do pravidel firewallu.

V závěru lze shrnout, že přínosy Flowmon Monitoring Center byly prakticky ověřeny na základě datových výstupů a analýz provozu. Systém prokázal schopnost detekovat relevantní provozní i bezpečnostní jevy, a poskytl správě IT konkrétní podklady pro optimalizaci sítě, vylepšení zásad přístupu i rychlejší reakce na incidenty.

Sběr a analýza síťového provozu

V testovaném prostředí univerzitní sítě byla pro účely monitorování a analýzy provozu využita toková data sbíraná pomocí protokolu NetFlow v9, který umožňuje export základních metadat o síťové komunikaci (např. IP adresy, porty, přenesený objem dat či protokol). Toky byly generovány na směrovačích a přepínačích třetí vrstvy a zasílány do Flowmon Collectoru, kde byly následně zpracovány modulem Monitoring Center.

Na rozdíl od hluboké inspekce paketů je toková analýza výhodná především nižšími nároky na úložiště a vyšší škálovatelností. V prostředí univerzitní sítě se tento přístup ukázal jako efektivní i při delším uchovávání záznamů – konkrétně 183 dní – a při pokrytí velkého počtu komunikujících zařízení.

Významným přínosem bylo i zachování souladu s legislativními normami, protože toková data pracují pouze s informacemi ze síťové a transportní vrstvy (OSI model), čímž se minimalizuje zpracování citlivých osobních údajů. Z hlediska GDPR byla tedy metoda zcela vyhovující i při použití v prostředí akademické instituce.

Pro detekci neobvyklého provozu byly tokové záznamy vizualizovány pomocí nástrojů Top Hosts, Top Protocols a Top Conversations. Z těchto přehledů bylo možné například určit nejvytíženější zařízení, monitorovat četnost DNS požadavků nebo zaznamenat intenzivní šifrovanou komunikaci mimo běžnou pracovní dobu, která následně sloužila jako vstup pro detekční modul ADS.

Z pohledu výkonu je významná i možnost optimalizace zpracování tokových dat pomocí DPDK (Vývojová sada pro zpracování dat) technologie, jak ji uvádí Zhang et al. (2018). Autoři prokázali, že implementace FlowMon DPDK umožňuje zpracovávat až několik milionů toků za sekundu, což je zásadní především v prostředí s vysokým zatížením a proměnlivou topologií, typickou právě pro univerzitní sítě.

Díky dlouhodobému uchovávání dat a nízké latenci zpracování bylo možné nejen odhalovat bezpečnostní hrozby, ale také sledovat dlouhodobé síťové trendy, optimalizovat infrastrukturu a identifikovat úzká místa. Toková analýza tak tvořila páteř celého monitorovacího řešení v síti Fakulty logistiky a krizového řízení.

Zdroje dat v testovaném prostředí

Sběr tokových dat v testovaném prostředí univerzitní sítě byl realizován prostřednictvím více zdrojů, které pokrývaly různé části infrastruktury s cílem získat co nejkomplexnější obraz o probíhající komunikaci. Klíčovými zařízeními, ze kterých byla data exportována, byly směrovače a přepínače třetí vrstvy (L3), které zajišťovaly směrování a filtrování provozu mezi jednotlivými VLAN a také mezi univerzitní sítí a veřejným internetem.

Hlavními zdroji tokových dat byly zařízení s IP adresami: 10.96.1.50, 10.96.1.51 a 10.32.26.66. Každé z těchto zařízení představovalo významný uzel v síťové infrastruktuře, zajišťující komunikaci mezi různými segmenty sítě. Byla tedy nastavena tak, aby

exportovala toková data protokolem NetFlow v9 na IP adresu kolektoru Flowmon (10.32.26.65) přes standardní port UDP 2055.

Směrovače a přepínače byly nakonfigurovány tak, aby toková data zahrnovala co nejvíce relevantních informací. Pro každý tok byly zaznamenávány atributy jako:

- Zdrojová a cílová IP adresa
- Zdrojový a cílový port
- Protokol (TCP, UDP, ICMP, atd.)
- Přenesený objem dat (bajty)
- Počet přenesených paketů
- VLAN ID (pokud byly použity)
- MAC adresy (v případě rozšířeného sběru dat)
- Příznaky TCP spojení (např. SYN, ACK, FIN)
- Délka trvání komunikace

Každé z těchto zařízení bylo zvoleno záměrně tak, aby pokrývalo různé části infrastruktury. Zařízení s IP adresou 10.96.1.50 sloužilo jako hlavní směrovač pro VLAN určené pro studentské laboratoře a učebny. Zařízení 10.96.1.51 pokrývalo administrativní a výzkumné segmenty sítě, včetně přístupových bodů Wi-Fi a serverových VLAN. Zařízení 10.32.26.66 bylo primárně využíváno pro komunikaci s externími službami a poskytovalo přístup k internetu pro celou fakultní síť.

Pro přenos tokových dat byla využita síťová rozhraní eth2 a eth3 na straně Flowmon kolektoru, přičemž obě rozhraní byla nastavena na plně duplexní režim s rychlostí 10 000 Mb/s. Bylo použito plné zachytávání toků (sampling rate: 0), což znamená, že všechna data byla zpracovávána bez vzorkování. Tato metoda byla zvolena, protože umožňuje přesnější detekci anomálií a lepší analýzu provozu.

V rámci rozšířených možností protokolu NetFlow v9 byly záznamy doplněny o informace týkající se DNS dotazů, TLS fingerprintů (JA3), protokolů vyšších vrstev (HTTP, SMB, DNS, DHCP) a dalších služeb běžících na aplikační vrstvě. Díky této konfiguraci bylo možné sledovat nejen základní síťové parametry, ale také aplikace a služby využívané v rámci fakultní sítě.

Toková data byla průběžně exportována v pětiminutových intervalech pomocí aktivních a neaktivních timeoutů (300 a 30 sekund). Toto nastavení umožňovalo pravidelně uzavírat toky, což zvyšovalo přesnost a konzistenci dat. Toky byly následně uloženy v interní databázi systému Flowmon Monitoring Center s nastavenou retencí 183 dní, což poskytovalo dostatečný časový horizont pro retrospektivní analýzu a detekci dlouhodobých trendů.

Tento komplexní sběr dat umožnil sledování komunikace napříč celou univerzitní sítí a poskytl dostatek informací pro detekci anomálií, zjištění výkonových problémů nebo zajištění bezpečnosti. Jak bylo později prokázáno, tento způsob sběru umožnil detekci potenciálních bezpečnostních incidentů, které by jinak nebyly zaznamenány běžnými monitorovacími prostředky.

Analýza základních síťových statistik

Po úspěšném nastavení sběru tokových dat a jejich uložení v systému Flowmon Monitoring Center bylo možné provést analýzu základních síťových statistik, které poskytly ucelený přehled o provozu v univerzitní síti. Tyto statistiky byly zaměřeny na identifikaci hlavních zdrojů a cílů komunikace, nejčastěji používaných protokolů, objemů přenesených dat a časových vzorců provozu.

Základní přehledy byly získány prostřednictvím nástrojů v modulu Flowmon Monitoring Center, které umožňují zobrazit data ve formě tabulek, grafů a časových řad. Analýza byla prováděna s ohledem na různé časové intervaly, aby bylo možné identifikovat jak krátkodobé události, tak i dlouhodobé trendy.

Top Hosts

Jedním z klíčových přehledů bylo sledování Top Hosts, které identifikovalo zařízení generující největší objemy provozu. Bylo zjištěno, že největší provoz byl generován servery umístěnými v administrativní VLAN, přičemž dominantní roli hrál zálohovací server zajišťující pravidelnou synchronizaci dat. Dále byly identifikovány i pracovní stanice zaměstnanců a zařízení připojená k Wi-Fi síti, zejména ve studentské VLAN.

Nárůst provozu byl pravidelně zaznamenáván v pracovních dnech mezi 7:45 a 13:00, což korespondovalo se začátkem výuky a jejím průběhem. Výrazný pokles nastával v odpoledních hodinách, zatímco během víkendů byla síťová aktivita minimální. Tento vzorec provozu odpovídá běžnému využití sítě v akademickém prostředí (Flowmon, 2023).

Top Protocols

Přehled Top Protocols poskytl informace o nejčastěji používaných protokolech. Ve sledovaném období dominovaly zejména protokoly TCP/443 (HTTPS), TCP/445 (SMB), UDP/53 (DNS) a TCP/80 (HTTP). Překvapivě vysoké množství provozu bylo zaznamenáno na portu TCP/445, což naznačovalo intenzivní využití SMB komunikace pro sdílení souborů mezi zařízeními.

V některých případech byly identifikovány také protokoly využívané pro vzdálený přístup, jako RDP a TeamViewer. Přítomnost těchto protokolů, zejména ve studentské VLAN, vyvolala podezření na neautorizovaný vzdálený přístup nebo na neformální používání nástrojů vzdálené správy (Cisco, 2023).

Top Conversations

Dalším důležitým přehledem bylo sledování Top Conversations, které umožnilo identifikovat nejvýznamnější komunikace mezi konkrétními zařízeními. Nejčastěji šlo o spojení mezi zálohovacími servery a pracovními stanicemi zaměstnanců v administrativní VLAN. Tento provoz probíhal převážně v nočních hodinách, což odpovídalo nastavenému harmonogramu záloh. Významné přenosy byly zaznamenány také mezi zařízeními v bezdrátové síti, zejména v období výuky, kdy studenti přistupovali k online zdrojům nebo vzdáleným službám.

V několika případech bylo zjištěno neobvyklé spojení mezi zařízeními umístěnými v různých VLAN, kde by neměla probíhat běžná komunikace. Tato situace vedla k dalšímu šetření v rámci bezpečnostní analýzy.

Top Applications

V rámci přehledu Top Applications bylo sledováno rozložení síťového provozu mezi jednotlivé aplikace a služby. Nejvýznamnější objem dat byl přenášen prostřednictvím HTTPS a DNS protokolů, což odpovídá běžnému akademickému využití sítě. Naopak nižší provoz byl generován aplikacemi jako VoIP, Samba nebo FTP, které byly používány jen výjimečně.

V některých případech byly detekovány aplikace, které nejsou oficiálně povolené, jako například BitTorrent nebo TOR, což vedlo ke zpřísnění bezpečnostních politik a následnému blokování těchto služeb.

Časová analýza

Důležitou součástí analýzy byla také časová korelace provozu. Pomocí grafů a časových řad bylo možné sledovat vývoj objemu komunikace v jednotlivých dnech a hodinách. Bylo zjištěno, že provoz kulminuje během výuky, zatímco ve večerních hodinách se výrazně snižuje. Výjimkou byly případy, kdy probíhaly zálohy nebo aktualizace zařízení, což způsobovalo dočasné nárůsty provozu v nočních hodinách.

Tato analýza základních síťových statistik poskytla důležitý náhled na strukturu a chování univerzitní sítě. Zjištěné údaje byly následně využity pro další bezpečnostní analýzy a optimalizaci provozu v síti. Na základě výsledků bylo možné provést úpravy v síťové architektuře, zlepšit politiky řízení přístupu a přesněji nastavit parametry pro detekci anomálií v dalších fázích testování.

Detekce provozních anomálií

Detekce provozních anomálií představuje klíčovou komponentu systému Flowmon Monitoring Center, která umožňuje odhalit nestandardní chování v síťovém provozu, jež může signalizovat potenciální bezpečnostní riziko nebo provozní problém. Tento proces spočívá v průběžném sledování tokových dat a jejich porovnávání s předem definovanými prahovými hodnotami či historickými vzory. Identifikované odchylky jsou pak klasifikovány jako anomálie, které mohou vyžadovat další analýzu nebo okamžitý zásah.

V testovaném prostředí univerzitní sítě bylo sledování anomálií prováděno prostřednictvím Flowmon ADS, který analyzoval veškeré toky přicházející do Flowmon Monitoring Center. Byly využívány různé detekční metody zaměřené na rozpoznání neobvyklého provozu, jako jsou náhlé nárůsty objemu dat, opakované pokusy o připojení, neobvyklá komunikace na nestandardních portech nebo případy nadměrné latence.

Nejčastěji byly detekovány následující typy provozních anomálií:

Náhlé zvýšení provozu – Bylo identifikováno zejména během zálohování dat v administrativní VLAN, kdy docházelo k výraznému nárůstu provozu v nočních hodinách. Tyto případy byly klasifikovány jako očekávané, avšak zvýšený provoz mimo běžnou pracovní dobu byl monitorován pro případné neautorizované přístupy.

Neukončená spojení (TCP retransmise) – Opakované pokusy o připojení, které nebyly úspěšně dokončeny, byly zaznamenány hlavně při komunikaci mezi zařízeními připojenými

prostřednictvím bezdrátových přístupových bodů. Tento jev mohl naznačovat problémy s konfigurací síťových zařízení, přetížení nebo rušení na fyzické vrstvě.

Komunikace na nestandardních portech – Několik zařízení ve studentské VLAN navazovalo spojení na neobvyklé porty, které nejsou standardně povoleny v síti. V Tabulka 6 lze tyto porty porovnat. Byly identifikovány především porty nad 50 000, což naznačovalo možnost zneužívání služeb nebo pokusů o skenování síťových prostředků.

Tabulka 6: Přehled protokolů a identifikovaných anomálií

Typ provozu/ Protokol	Popis anomálie	Možné příčiny
Zvýšený noční provoz (TCP/ SMB)	Zvýšený objem dat mezi 22:00 a 6:00 zejména ve VLAN administrativy	Zálohování neautorizované přenosy, skripty běžící mimo pracovní dobu
Neukončená spojení (TCP retransmise)	Opakované retransmise TCP spojení, časté u WI-FI, přístupových bodů	Nestabilní WI-FI připojení, rušení, chybná konfigurace zařízení
Nestandardní porty (TCP > 50 000)	Komunikace na nepovolené porty, podezření na skenování nebo P2P aktivity	Obcházení pravidel firewallu, využívání P2P nebo proxy služeb
DNS dotazy (UDP/ 53)	Nadměrný počet DNS dotazů během krátké doby, možný DNS tunneling	Zneužití DNS pro skrytou komunikaci, malware aktivita

(zdroj: vlastní)

DNS Anomálie – Modul DNS Anomaly upozorňoval na nestandardní DNS dotazy směřující na neznámé nebo podezřelé domény. V některých případech bylo zaznamenáno nadměrné množství dotazů během krátké doby, což mohlo svědčit o pokusu o DNS tunneling nebo jiné formy zneužití služeb.

Neobvyklý provoz v síti hostů – V rámci segmentu VLAN určeného pro hosty byly zaznamenány výrazné nárůsty přeneseného objemu dat, které překračovaly stanovené limity. Tento provoz probíhal zejména v nočních hodinách, což bylo vyhodnoceno jako možné zneužití přístupu nebo nesprávná konfigurace přístupových pravidel.

Jedním z nástrojů, který výrazně pomohl při identifikaci těchto anomálií, byla možnost generování přehledů ve Flowmon Monitoring Center, kde byly prezentovány informace o „Top Hosts“, „Top Protocols“ a „Top Conversations“. Pomocí těchto přehledů bylo možné detailně sledovat, která zařízení generují podezřelý provoz a jaké aplikace nebo protokoly jsou při tom využívány. Přehled těchto detekovaných anomálií se nachází v Tabulka 7.

Tabulka 7: Přehled detekovaných anomálií

Typ anomálie	Popis	Kategorizace
Náhlé zvýšení provozu	Identifikováno během zálohování dat, výrazný nárůst provozu zejména v noci	Očekávaná (sledována pro jistotu)
Zvýšený provoz mimo pracovní dobu	Zaznamenány velké objemy přenosů ve večerních a nočních hodinách	Podezřelá (vyžaduje pozornost)
Neobvyklá komunikace na nestandardních portech	Detekovaná komunikace na neobvyklých portech (např. >50 000)	Možná hrozba (další analýza nutná)
Opakované pokusy a připojení	Zaznamenány časté pokusy o připojení k určitému serveru	Podezřelá (možný brute-force)
Nadměrná latence	Zpomalení odezvy některých služeb, zejména ve špičkách	Provozní problém (nutná optimalizace)

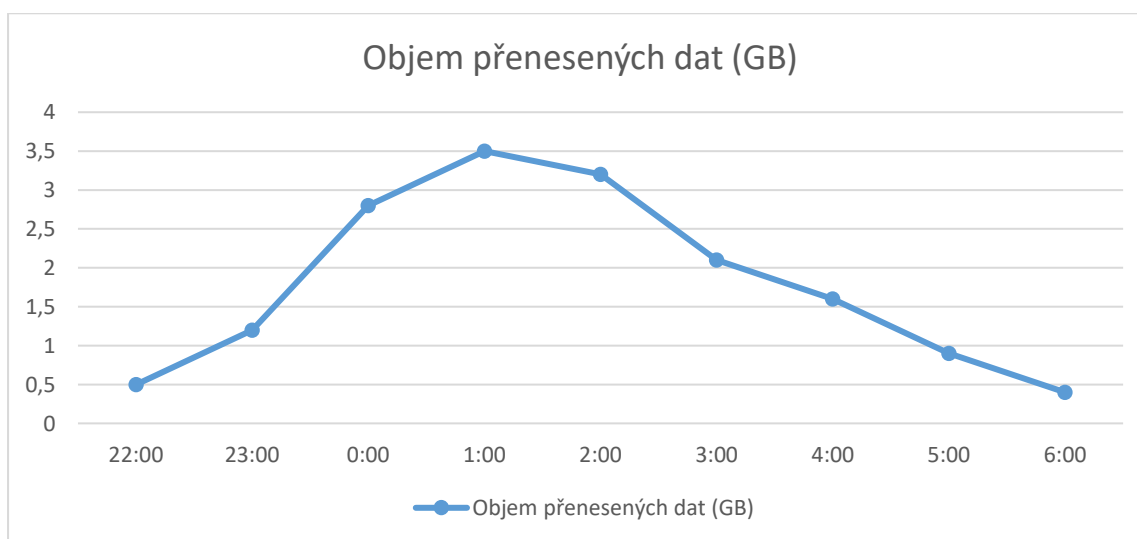
(zdroj: vlastní)

Bezpečnostní podezření z provozní analýzy

Prostřednictvím modulu Flowmon Monitoring Center byly odhaleny i situace, které naznačovaly možné bezpečnostní hrozby či neobvyklé aktivity v rámci univerzitní sítě. Přestože Monitoring Center není primárně zaměřeno na aktivní detekci kybernetických útoků, jeho analytické schopnosti umožňují odhalit nestandardní vzorce komunikace, které mohou indikovat bezpečnostní incidenty. Tyto jevy byly následně předány k hlubší analýze v modulu Flowmon ADS.

V jednom z případů bylo identifikováno podezřelé chování v rámci studentské VLAN, kde bylo zaznamenáno neobvykle velké množství přenesených dat směrem do externího cloudového úložiště během nočních hodin. Na základě analýzy přehledu „Top Conversations“ bylo zjištěno, že některá zařízení pravidelně odesílala data o velikosti několika gigabajtů v době, kdy nemělo probíhat žádné plánované zálohování ani synchronizace. Tato komunikace probíhala převážně přes šifrované spojení (protokol TCP/443), což znemožnilo její detailní analýzu na úrovni obsahu. Podezření na možné využívání VPN nebo jiných nástrojů pro utajení provozu bylo předáno k hlubší kontrole pomocí heuristických metod v modulu ADS.

Na Obrázek 1 se zobrazuje detekce podezřelé komunikace přes šifrované spojení (TCP/443) v průběhu 24 hodin. Patrné jsou neobvyklé špičky přenosů v nočních hodinách, které mohou signalizovat neoprávněné stahování nebo synchronizaci velkých objemů dat mimo standardní provozní dobu.



Obrázek 1: Detekce podezřelé komunikace přes šifrované spojení (TCP/443)

(zdroj: vlastní)

Další podezření se týkalo opakovaných DNS dotazů, které byly směřovány na domény neznámého původu nebo dokonce na neveřejné domény. V některých případech byly detekovány stovky dotazů během krátkého časového úseku, což mohlo svědčit o přítomnosti malware, který využíval DNS tunneling k přenosu dat nebo k neautorizované komunikaci s externími servery. Tento jev byl identifikován metodou DNS Anomaly, která byla následně aplikována v modulu ADS pro důkladnější vyhodnocení.

Za bezpečnostně relevantní bylo rovněž považováno opakované skenování síťových portů z některých externích IP adres. Pomocí přehledu „Top Ports“ bylo možné sledovat, že cílem útoků byly především otevřené porty využívané pro vzdálený přístup (RDP, SSH) nebo pro přenos souborů (FTP, SMB). K těmto aktivitám docházelo především v noci nebo během víkendů, kdy byla síťová aktivita jinak minimální. Pomocí integrace s blacklisty bylo zjištěno, že některé z těchto IP adres byly již dříve označeny jako podezřelé, což potvrdilo potřebu nasazení ochranných opatření.

Specifickým případem byla detekce opakované komunikace s IP adresami, které byly zahrnuty na blacklistech veřejných bezpečnostních databází. Tento typ detekce je součástí metodiky BLACKLIST, která umožňuje automatické označení podezřelé komunikace na základě porovnání s databází škodlivých IP adres. V několika případech se ukázalo, že komunikace pocházela ze zařízení, která byla připojena přes bezdrátovou síť pro hosty, což zvýšilo riziko neautorizovaných přístupů nebo šíření škodlivého softwaru.

5.2 Flowmon ADS

Modul Flowmon ADS je klíčovou součástí celého řešení Flowmon, která se zaměřuje na detekci neobvyklého a potenciálně nebezpečného chování v síťovém provozu. Na rozdíl od tradičních systémů IDS/IPS, které spoléhají především na signatury známých útoků, Flowmon ADS využívá behaviorální analýzu a pokročilé algoritmy strojového učení k identifikaci anomálií v reálném čase. Tento přístup umožňuje detekci nových, dosud neznámých hrozeb.

Princip fungování modulu Flowmon ADS je založen na nepřetržitém monitorování síťového provozu a vyhodnocování síťových toků (NetFlow, IPFIX). ADS se nezaměřuje na obsah paketů, ale na jejich metainformace – zdrojové a cílové IP adresy, porty, protokoly, objemy přenesených dat a časové charakteristiky komunikace. Na základě těchto atributů jsou generovány a analyzovány jednotlivé toky, které jsou následně porovnávány s definovanými modely chování.

Flowmon ADS využívá několik detekčních metod, které lze rozdělit na dvě základní skupiny – metody statické a dynamické. Statické metody jsou založeny na předem definovaných pravidlech a heuristikách, které jsou vytvářeny na základě známých bezpečnostních hrozeb a běžného chování síťových protokolů. Dynamické metody naopak využívají pokročilou analýzu založenou na strojovém učení a adaptivních modelech. Tyto metody umožňují průběžné učení a přizpůsobování systému specifikům sledované sítě.

Každá detekční metoda v systému Flowmon ADS je zaměřena na konkrétní typ anomálie. Například metoda BruteForce detekuje opakované pokusy o přihlášení k různým službám, metoda DNSAnomaly identifikuje nestandardní DNS dotazy, které mohou být příznakem DNS tunnelingu nebo C&C (Řídící a kontrolní) komunikace. Další důležité metody zahrnují například PortScan, DDoS Detection, UPLOAD nebo AlienDev – každá z nich je specializovaná na určité chování nebo typ hrozby.

Detekce je prováděna na základě korelace mezi historickými a aktuálními daty. Flowmon ADS si vytváří vlastní modely chování na základě dlouhodobě sledovaných toků, které jsou ukládány v databázi Flowmon Monitoring Center. Díky tomu je možné nejen detekovat aktuální hrozby, ale také vyhodnocovat dlouhodobé trendy a identifikovat například postupný laterální pohyb útočníků v síti.

Důležitou vlastností modulu Flowmon ADS je také možnost integrace s dalšími bezpečnostními nástroji. Výstupy ADS lze exportovat do SIEM systémů nebo použít jako vstupy pro automatizované reakce v rámci firewallů nebo dalších ochranných mechanismů. Tato schopnost umožňuje nejen detekovat hrozby, ale i na ně okamžitě reagovat a případně blokovat škodlivý provoz přímo na úrovni síťové infrastruktury.

Velkou výhodou je i schopnost upravovat citlivost jednotlivých detekčních metod a možnost definovat vlastní pravidla, což umožňuje přizpůsobení systému konkrétnímu prostředí. Detekční metody mohou být nastaveny ve třech režimech citlivosti: konzervativní, standardní a agresivní. Tento přístup umožňuje vyvážit přesnost detekce s mírou falešně pozitivních hlášení.

V praktickém nasazení v univerzitní síti se Flowmon ADS ukázal jako efektivní nástroj schopný odhalit nejen bezpečnostní incidenty, ale také nestandardní provozní chování, které může mít vliv na výkon nebo dostupnost služeb. Následující kapitola se zaměřuje na konkrétní detekční metody a jejich aplikaci při sledování univerzitní sítě.

Nasazení ADS v testovaném prostředí

Modul Flowmon ADS byl v testovaném prostředí univerzitní sítě nasazen jako součást systému Flowmon Monitoring Center. Tento modul byl integrován s tokovými daty poskytovanými prostřednictvím protokolu NetFlow v9, které byly exportovány z klíčových zařízení v síti – především směrovačů a L3 přepínačů, jak bylo uvedeno v předchozích kapitolách. Toková data byla přijímána prostřednictvím dvou aktivních monitorovacích rozhraní (eth2 a eth3) a dále zpracovávána modulem ADS, který zajišťoval jejich analýzu v reálném čase.

Nasazení ADS bylo provedeno přímo v prostředí Flowmon Monitoring Center, které sloužilo jako centrální rozhraní pro konfiguraci a sledování bezpečnostních incidentů. Modul byl aktivován prostřednictvím webového rozhraní a propojen s tokovými daty, které byly již dříve shromažďovány a archivovány. Hlavní výhodou tohoto řešení byla skutečnost, že nebylo nutné nasazovat žádné dodatečné senzory nebo fyzická zařízení. ADS pracoval s existujícími tokovými daty, což zjednodušilo jeho implementaci i správu.

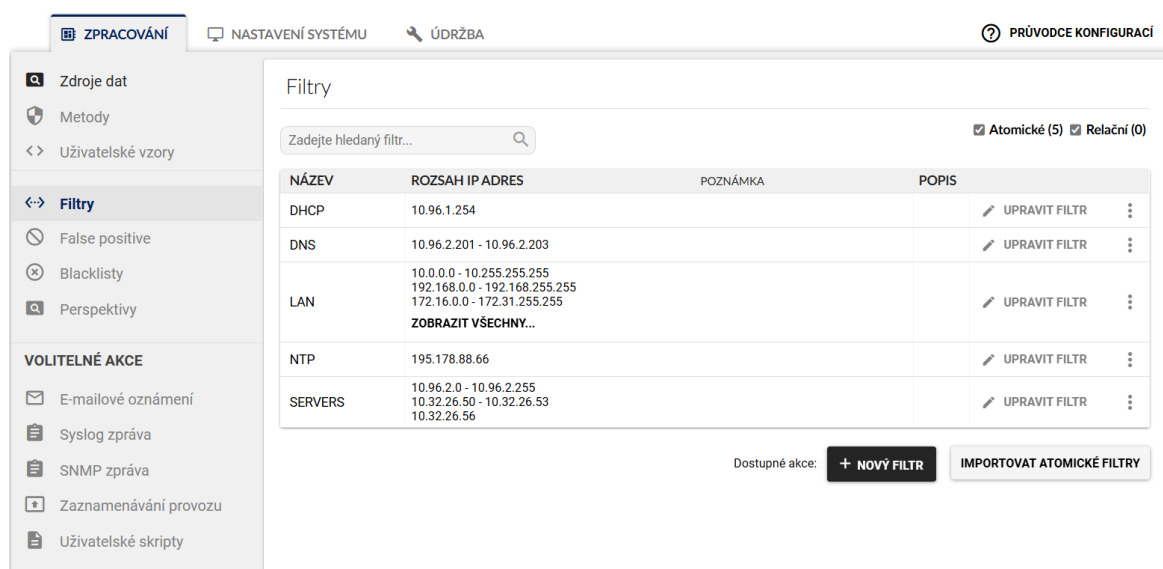
Po aktivaci modulu byly nastaveny detekční metody podle charakteristik univerzitní sítě. Byly aktivovány zejména následující metody:

- **BruteForce** – Detekce opakovaných pokusů o přihlášení z různých IP adres, což bylo považováno za potenciální pokus o prolomení hesel.
- **DNSAnomaly** – Vyhodnocování nestandardních DNS dotazů, které by mohly naznačovat DNS tunneling nebo komunikaci s C&C servery.
- **PortScan** – Identifikace pokusů o skenování portů, a to jak horizontálního (více portů na jedné IP adrese), tak vertikálního (jeden port na více IP adresách).
- **DDoS Detection** – Monitorování náhlých nárůstů přenosů nebo nadměrného počtu požadavků z jedné IP adresy, které mohou indikovat probíhající DDoS útok.
- **UPLOAD** – Detekce neobvykle velkých výstupních přenosů, což by mohlo znamenat exfiltraci dat nebo jiné neautorizované operace.

Nastavení jednotlivých metod bylo přizpůsobeno potřebám univerzitní sítě. Pro každý detekční algoritmus byly definovány prahové hodnoty, které odpovídaly běžnému provozu. Tento přístup umožnil minimalizovat výskyt falešně pozitivních hlášení a zároveň zajistit, že skutečné hrozby budou identifikovány včas.

Modul ADS byl v rámci testovaného prostředí konfigurován ve standardním režimu citlivosti. Tento režim umožňuje kombinovat detekční metody s různou úrovní přísnosti, čímž se zajišťuje optimální rovnováha mezi přesností detekce a minimalizací falešně pozitivních hlášení. Systém poskytoval možnost přepnutí do konzervativního nebo agresivního režimu, což bylo doporučeno pro situace vyžadující zvýšenou citlivost nebo naopak vyšší toleranci k běžným odchylkám.

Důležitým krokem v konfiguraci modulu ADS bylo nastavení notifikací a exportu zjištěných incidentů. Flowmon ADS umožňoval automatické generování varování při detekci závažných hrozeb. Tato varování byla následně odesílána prostřednictvím e-mailu nebo Syslog zpráv, což umožňovalo jejich integraci s dalšími bezpečnostními nástroji, například s SIEM systémy. Obrázek 2 poukazuje na konfigurace filtrů, které definují sledované rozsahy IP adres a typy provozu.



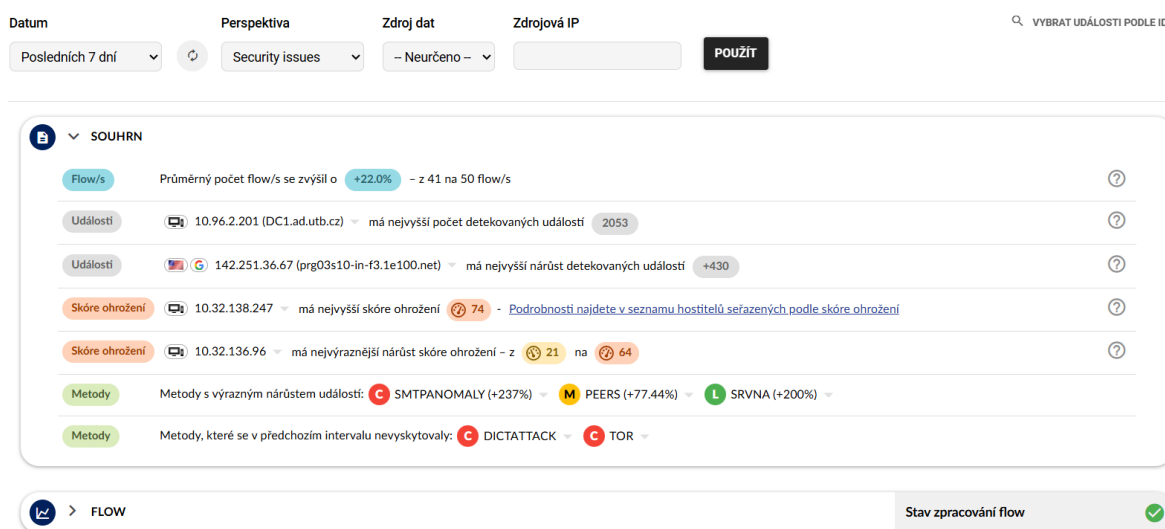
Obrázek 2: Konfigurace atomických filtrů

(zdroj: vlastní)

Průběh detekce byl průběžně monitorován v rámci administračního rozhraní, kde bylo možné sledovat seznam aktuálních i historických incidentů, jejich klasifikaci a detaily o způsobu detekce. Každý incident obsahoval podrobný popis, který zahrnoval například IP adresy, porty, časové údaje a závažnost incidentu.

Typy detekovaných anomálií

Modul Flowmon ADS umožňuje detekci široké škály anomálií, které jsou identifikovány na základě behaviorální analýzy tokových dat a heuristických metod. Na Obrázek 3 lze spatřit detekované události a anomálie. V testovaném prostředí univerzitní sítě byly identifikovány různé druhy anomálií, které zahrnovaly jak bezpečnostní hrozby, tak provozní problémy. Typy detekovaných anomálií lze rozdělit do několika hlavních kategorií, přičemž každá z nich je detekována pomocí specifických metod implementovaných v modulu ADS.



Obrázek 3: Souhrn detekovaných událostí a anomálií

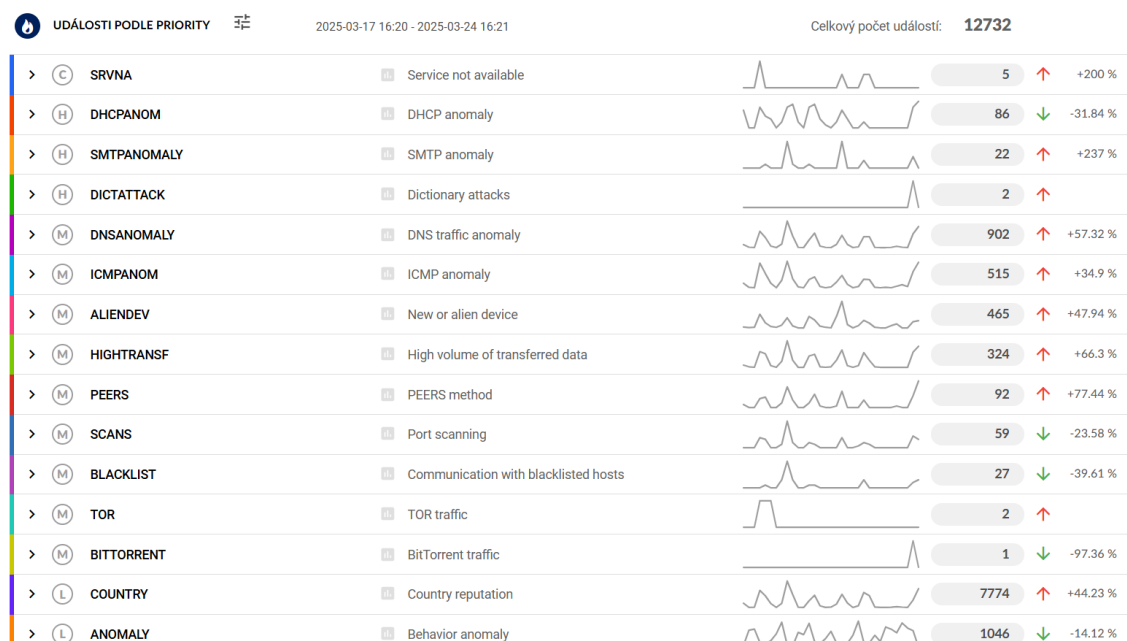
(zdroj: vlastní)

Jedním z nejčastěji detekovaných typů anomálií byly útoky typu BruteForce, které byly identifikovány na základě opakovaných pokusů o připojení k serverům na specifických portech (např. RDP, SSH). Modul Flowmon ADS identifikoval podezřelý provoz, kdy došlo k rychlému opakovanému odeslání požadavků s cílem získat přístup k cílovým zařízením. Tento typ útoku byl nejčastěji registrován v segmentu sítě určeném pro laboratorní zařízení, kde byla povolena komunikace přes SSH protokol.

Další významnou kategorií byly anomálie související s přenosem velkého objemu dat. Tento typ detekce byl realizován metodami jako UPLOAD nebo Hightransf, které sledovaly objem datových přenosů překračujících stanovené limity. V několika případech bylo zjištěno, že dochází k nadměrnému přenosu dat z vybraných pracovních stanic do externích cloudových služeb mimo běžnou pracovní dobu. Tato skutečnost mohla naznačovat neoprávněné zálohování nebo přenos citlivých informací mimo zabezpečené prostředí.

Pomocí metody DNS Anomaly byly detekovány nestandardní DNS dotazy, které mohly ukazovat na komunikaci s C&C servery nebo využívání DNS tunelování. V několika případech bylo zaznamenáno, že zařízení opakovaně zasílá dotazy na domény, které nebyly běžně využívány ani registrovány v DNS záznamech univerzity. Tento typ provozu mohl indikovat pokus o obcházení firewallu nebo skrytý přenos dat prostřednictvím DNS.

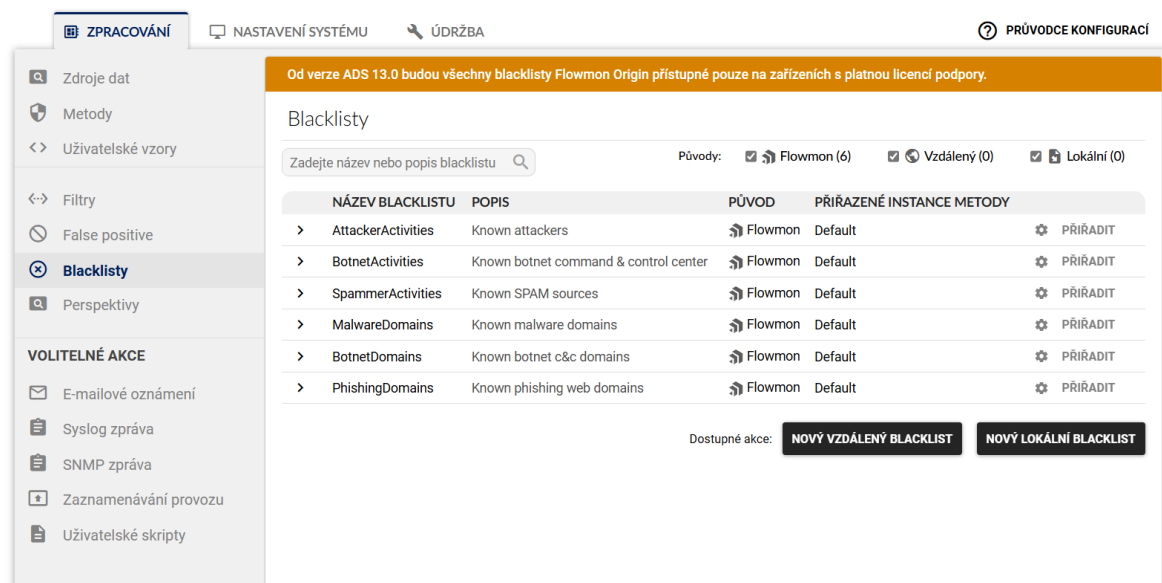
Velmi často se také objevovaly incidenty spojené se skenováním portů a neautorizovanými pokusy o připojení. Tyto aktivity byly identifikovány pomocí metod AlienDev a Portscan, které sledují počet pokusů o připojení na různé porty během krátkého časového období. V testovaném prostředí byla taková aktivita často detekována zejména ve VLAN určené pro přístup hostů, kde bylo připojeno velké množství zařízení s neznámou bezpečnostní politikou. Seznam detekovaných anomálií lze shlédnout na Obrázek 4.



Obrázek 4: Seznam detekovaných anomálií v období 17.–24. března 2025 – trend výskytu

(zdroj: vlastní)

Další typ detekovaných anomálií zahrnoval neautorizovaný přístup k citlivým službám. Pomocí metody BLACKLIST ukazuje Obrázek 5, bylo zjištěno, že některá zařízení komunikují s IP adresami uvedenými na veřejných blacklistových seznámech. Ačkoli se většinou jednalo o krátkodobá spojení způsobená nesprávně nakonfigurovanými aplikacemi, v několika případech bylo zjištěno podezřelé spojení, které si vyžádalo následnou analýzu.

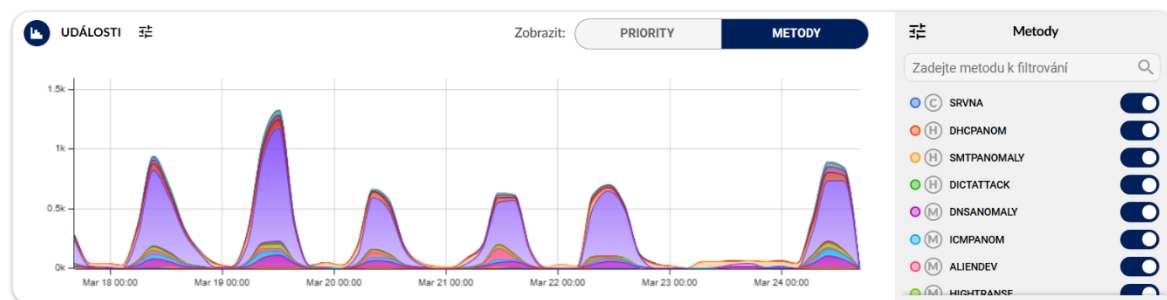


Obrázek 5: „Blacklisty“

(zdroj: vlastní)

Významnou část detekovaných incidentů tvořily i anomaly spojené s připojením k externím službám. Typicky se jednalo o pokusy o připojení přes VPN nebo RDP mimo standardní pracovní dobu. Tento typ anomálie byl monitorován pomocí metod DstLocation a ExternalAccess, které sledují komunikaci směřující mimo definovaný rozsah IP adres nebo do geograficky vzdálených lokalit.

Všechny výše uvedené typy detekovaných anomálií byly podrobně analyzovány v rámci modulu Flowmon ADS, kde bylo možné sledovat časový průběh incidentu, jak lze vidět na Obrázek 6, konkrétní IP adresy a další související informace. Díky možnosti integrace s ostatními komponentami Flowmonu bylo možné incidenty zpětně dohledat, potvrdit nebo vyhodnotit jako falešně pozitivní.



Obrázek 6: Časová osa detekovaných bezpečnostní metod v období 18.–24. března 2025

(zdroj: vlastní)

Příklady konkrétních bezpečnostních událostí

V rámci testování modulu Flowmon ADS byly detekovány různé bezpečnostní události, které poskytly ucelený přehled o potenciálních hrozbách a anomáliích v univerzitní síti. V následujících případech jsou popsány konkrétní incidenty zachycené během monitorování a způsob jejich detekce.

Jedním z často opakujících se incidentů byly pokusy o neautorizovaný přístup přes protokol SSH. Flowmon ADS detekoval zvýšený počet pokusů o navázání spojení na standardním portu TCP/22 z IP adres, které nebyly součástí univerzitní sítě. Tento typ útoku byl identifikován metodou BruteForce, která monitoruje abnormální počet pokusů o přihlášení během krátkého časového intervalu, jak lze vidět na Obrázek 7. Výsledky byly klasifikovány jako vysoké riziko, neboť takový druh útoku může vést k získání neautorizovaného přístupu k citlivým systémům.

Datum	Perspektiva	IP adresy		
Posledních 7 dní	Security issues		POUŽÍT	VÍCE FILTRŮ...
JEDNODUCHÝ SEZNAM	PODLE MITRE ATT&CK	PODLE ZAŘÍZENÍ	AGREGOVANÝ POHLED	
> 74	10.32.138.247 (neznámá)	Zdrojem události: 155	Cílem události: 70	
> 67	10.32.132.156 (neznámá)	Zdrojem události: 137	Cílem události: 98	
> 65	10.32.131.112 (neznámá)	Zdrojem události: 81	Cílem události: 107	
> 64	10.32.136.96 (neznámá)	Zdrojem události: 97	Cílem události: 15	
> 64	10.32.135.25 (neznámá)	Zdrojem události: 75	Cílem události: 28	
> 63	10.32.143.155 (neznámá)	Zdrojem události: 73	Cílem události: 38	
> 63	10.32.138.26 (neznámá)	Zdrojem události: 138	Cílem události: 14	
> 63	10.32.130.169 (neznámá)	Zdrojem události: 58	Cílem události: 84	
> 63	10.32.130.97 (neznámá)	Zdrojem události: 145	Cílem události: 130	
> 62	10.32.133.183 (neznámá)	Zdrojem události: 90	Cílem události: 14	
> 62	10.32.129.134 (neznámá)	Zdrojem události: 136	Cílem události: 48	

Obrázek 7: Přehled zařízení podle skóre ohrožení a detekovaných událostí

(zdroj: vlastní)

Dalším příkladem byla detekce tzv. DNS Tunnelingu. Tento typ útoku využívá běžné DNS dotazy k přenosu škodlivých dat nebo ke skrytí komunikace s kontrolními servery. Modul Flowmon ADS zaznamenal velké množství neobvyklých DNS dotazů z jedné pracovní stanice, které směřovaly na podezřelé nebo neexistující domény. Metoda DNSAnomaly zaznamenala nejen zvýšený počet požadavků, ale také nestandardní strukturu DNS dotazů, což indikovalo možný pokus o tunelování nebo C&C komunikaci.

Dalším významným incidentem byl detekován pokus o tzv. DDoS útok. Flowmon ADS identifikoval vysoký počet připojení na konkrétní IP adresu během velmi krátkého časového úseku. Analýza přehledů v Monitoring Center potvrdila, že provoz byl generován z několika různých IP adres, což mohlo naznačovat buď přímý útok na univerzitní server, nebo jeho zneužití v rámci většího distribuovaného útoku.

V průběhu monitorování byly rovněž identifikovány případy neautorizovaného využívání protokolu RDP. Některé pracovní stanice byly připojeny na neznámé externí IP adresy prostřednictvím portu TCP/3389. Modul Flowmon ADS detekoval tyto pokusy na základě metody AlienDev, která sleduje komunikaci se zařízeními, která nejsou standardně přítomna v síti. Toto chování bylo následně označeno jako vysoce rizikové, neboť přístup přes RDP může vést k přímému ovládnutí zařízení.

Všechny výše zmíněné události byly zaznamenány a vyhodnoceny prostřednictvím Flowmon ADS. Systém umožnil nejen detekci těchto incidentů, ale také jejich kategorizaci a další analýzu, na Obrázek 8 můžeme vidět přehled konkrétních bezpečnostních událostí. Ve všech případech bylo možné okamžitě reagovat a minimalizovat potenciální škody.

Datum

Perspektiva

Zdrojová IP

Cíle

POUŽÍT

VÍCE FILTRů...

JEDNODUCHÝ SEZNAM

PODLE MITRE ATT&CK

PODLE ZAŘÍZENÍ

AGREGOVANÝ POHLED

EXPORTOVAT UDÁLOSTI DO SOUBORU CSV

OTEVŘÍT V NOVÉ KARTĚ

#	ID	ČAS DETEKCE	TYP UDÁLOSTI	PODTPY UDÁLOSTI	ZDROJ	DETAIL
1	#1532047	2025-03-24 16:28:52	COUNTRY	IncreasedCommunication	10.32.142.193	Neobvyklá komunikace do země Germany: zařízení: 6.18 MiB, staženo: 8.87 MiB, poměr nahráno/staženo: 0.696; průměrné nahráno/staženo: 230.73 KiB, staženo: 998.15 KiB, poměr nahráno/staženo: 0.231).
2	#1532045	2025-03-24 16:28:48	COUNTRY	IncreasedCommunication	10.32.142.193	Neobvyklá komunikace do země (nahráno: 24.36 MiB, staženo: 411.75 KiB, poměr nahráno/staženo: 60.59; průměrné nahráno/staženo: 217.55 KiB, staženo: 410.74 KiB, poměr nahráno/staženo: 0.529).
3	#1532039	2025-03-24 16:28:36	ALIENDEV	IPBased	10.32.128.98	Nové zařízení (MAC adresa: 10:6F:D9:BF:FE:FE) detekováno na základě své IP adresy.
4	#1532038	2025-03-24 16:28:36	ALIENDEV	MACBased	fe80::126f:d9ff:feb9:896f	Nové zařízení (MAC adresa: 10:6F:D9:BF:FE:FE) detekováno na základě své MAC adresy.
5	#1532030	2025-03-24 16:28:20	DNSANOMALY	TCPHighTraffic	10.32.142.39	Přeneseno velké množství TCP DNS provozu: data: 8.31 KiB, přijatá data: 9.9 KiB.
6	#1532028	2025-03-24 16:28:16	COUNTRY	IncreasedCommunication	10.32.134.185	Neobvyklá komunikace do země (nahráno: 1.05 MiB, staženo: 267.26 KiB, poměr nahráno/staženo: 4.038; průměrné nahráno v síti: 71.1 KiB, staženo: 364.84 KiB, poměr nahráno/staženo: 0.19).

Obrázek 8: Přehled konkrétních bezpečnostních událostí

(zdroj: vlastní)

Vyhodnocení funkčnosti ADS

Pro systematické vyhodnocení rizik spojených s provozem a konfigurací modulu Flowmon ADS byla využita metoda FMEA. V rámci této analýzy byl každý identifikovaný problém

hodnocen z pohledu tří základních parametrů. Závažnost (Severity) – jak velký dopad má daný problém na funkčnost systému či bezpečnost sítě. Četnost výskytu (Occurrence) – jak často k danému selhání dochází nebo může docházet. Odhalitelnost (Detection) – jak snadno lze dané riziko identifikovat dříve, než způsobí problém.

Tyto tři faktory jsou násobeny a výsledkem je tzv. Risk Priority Number (RPN) – číselný ukazatel, který slouží k určení priorit při řešení jednotlivých hrozeb. Čím vyšší RPN, tím závažnější a akutnější dané riziko je.

Výsledky analýzy FMEA ukázaly několik klíčových problémových oblastí v rámci využívání modulu Flowmon ADS v akademickém prostředí. V Tabulka 8 lze pozorovat tyto výsledky. Nejvýznamnějším z nich byly falešně pozitivní detekce, které vykazovaly vysoké skóre RPN (210). Tento jev se ukázal jako mimořádně problematický především v souvislosti s vyšším počtem incidentů, které bylo nutné ručně ověřovat, což vedlo k zatížení pracovníků zajišťujících bezpečnost sítě. Projevovalo se to zejména v situacích, kdy byl systém konfigurován v citlivějším režimu, a tedy více reagoval i na běžné provozní odchylky.

Dalším důležitým zjištěním bylo zjištění zvýšené latence při analýze síťového provozu, především v obdobích vysokého zatížení sítě. Tato latence může vést ke zpoždění detekce kritických incidentů, což snižuje schopnost systému reagovat v reálném čase. U tohoto rizika bylo identifikováno $RPN = 168$, a to zejména kvůli nedostatečnému výkonu výpočetních prostředků v kombinaci s vysokým objemem analyzovaných toků.

Další významné riziko představovalo nezachycení komunikace probíhající na neznámých portech, typicky využívaných pokročilými typy malware nebo nástroji pro obcházení běžných detekčních mechanismů. Toto riziko ($RPN = 160$) se ukázalo jako důležité zejména při analýze chování zařízení v méně sledovaných částech sítě, kde může snadno dojít k neautorizovaným přístupům nebo ke zneužití zranitelností bez povšimnutí.

V analýze byla také identifikována hrozba ztráty UDP toků při přetížení, což může mít negativní vliv na detekci DDoS útoků nebo jiných typů anomálního chování. Jelikož UDP protokol není spojově orientovaný, jeho ztráta může snadno uniknout pozornosti, a tím pádem i správné interpretaci v rámci ADS. Tento problém dosáhl $RPN 150$.

Konečně posledním sledovaným rizikem bylo nedetekování DDoS útoku v případě nízkého počtu spojení, tedy scénář, kdy útočník využívá menší objemy spojení k zahlcení služby.

Tento typ útoku je obtížněji detekovatelný tradičními metodami, a proto dosáhl hodnoty RPN = 108.

Všechny uvedené nedostatky byly klasifikovány jako střední až vysoká rizika a byla navržena konkrétní opatření ke zmírnění jejich dopadů, včetně úprav konfigurace detekčních pravidel, posílení hardwarové infrastruktury, pravidelné aktualizace signatur a využití adaptivních metod analýzy provozu.

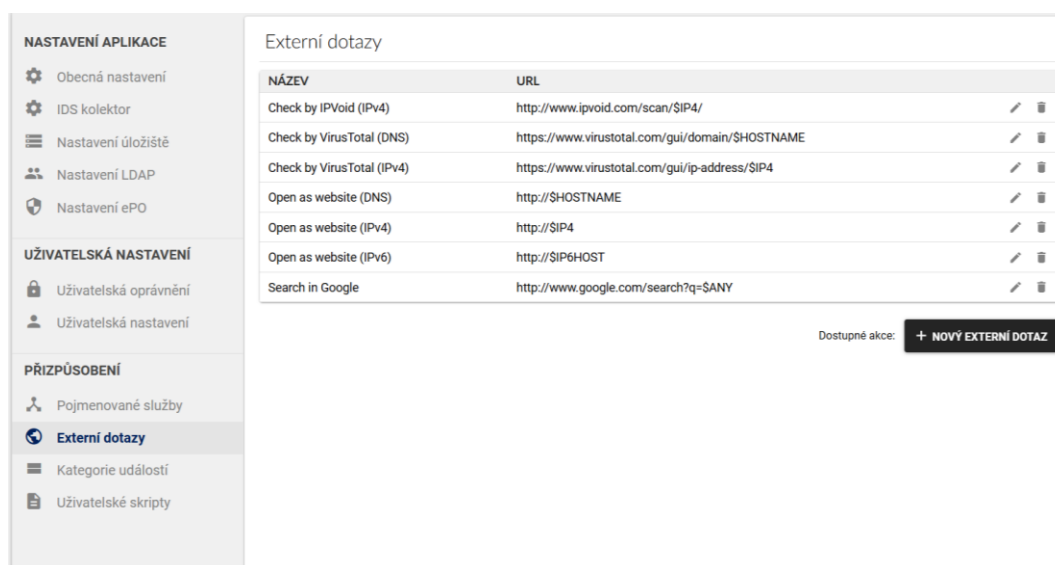
Tabulka 8: FMEA analýza modulu Flowmon ADS

Riziko	Příčina	Důsledek	Výskyt (O)	Závažnost (S)	Odhalitelnost (D)	RPN
Falešné pozitivní detekce	Nesprávné nastavení detekční citlivosti	Zbytečná eskalace incidentů	7	6	5	210
Zvýšená latence analýzy	Nedostatečný výkon při špičkovém zatížení	Zpoždění v reakci na hrozbu	6	7	4	168
Ztráta UDP toků	Vysoká datová zátěž	Nepřesná data v analýze	5	5	6	150
Nezachycené spojení na neznámý port	Port není definován v signatuře	Možný přístup útočníka	4	8	5	160
Nedetekovaný DDoS útok	Nízký počet aktivních spojení	Nezabráněný útok na dostupnost služby	3	9	4	108

(zdroj: vlastní)

Modul Flowmon ADS byl v testovaném prostředí nasazen s cílem detekovat široké spektrum bezpečnostních hrozeb, které by mohly ohrozit stabilitu a bezpečnost univerzitní sítě. Testování se zaměřilo především na schopnost systému detekovat jak známé typy útoků, tak i anomální chování, které by mohlo ukazovat na dosud neznámé hrozby.

Flowmon ADS prokázal svou efektivitu především při detekci opakovaných pokusů o přístup pomocí protokolu SSH (metoda BruteForce), kde dokázal odhalit neautorizované pokusy o přihlášení z externích IP adres. Externí dotazy lze vidět na Obrázek 9. Výhodou této metody byla schopnost detekce nejenom na základě četnosti pokusů, ale také v kontextu časové analýzy a rozpoznání dlouhodobějších útoků, které by mohly být jinak přehlédnuty.



NÁZEV	URL
Check by IPVoid (IPv4)	http://www.ipvoid.com/scan/\$IP4/
Check by VirusTotal (DNS)	https://www.virustotal.com/gui/domain/\$HOSTNAME
Check by VirusTotal (IPv4)	https://www.virustotal.com/gui/ip-address/\$IP4
Open as website (DNS)	http://\$HOSTNAME
Open as website (IPv4)	http://\$IP4
Open as website (IPv6)	http://\$IP6HOST
Search in Google	http://www.google.com/search?q=\$ANY

Dostupné akce: + NOVÝ EXTERNÍ DOTAZ

Obrázek 9: Seznam externích dotazů

(zdroj: vlastní)

Modul byl rovněž úspěšný při identifikaci neobvyklých DNS dotazů pomocí metody DNSAnomaly. V tomto případě byly detekovány pokusy o DNS Tunneling, kdy byla běžná DNS komunikace zneužita ke skryté výměně dat. Tento typ analýzy je důležitý zejména v akademickém prostředí, kde může být zneužit ke krádeži citlivých dat nebo k exfiltrování informací přes nechráněné DNS servery.

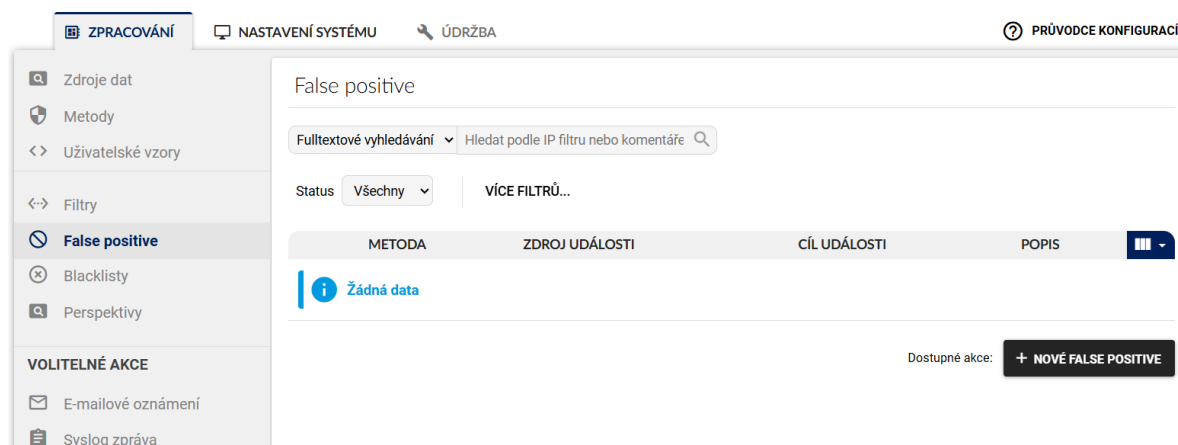
Dalším pozitivním výsledkem bylo zachycení distribuovaných útoků DDoS, kde Flowmon ADS dokázal identifikovat zvýšený počet připojení na konkrétní IP adresu. Díky metodě **DoSAttack** bylo možné odlišit běžné provozní špičky od skutečných útoků, což je klíčové pro zajištění dostupnosti kritických služeb. Výhodou byla i možnost vizualizace tohoto jevu

v rámci Monitoring Center, kde byly zobrazeny veškeré související toky a jejich charakteristiky.

Prostřednictvím metody AlienDev byla zjištěna také nestandardní komunikace využívající vzdálený přístup přes RDP. Modul ADS správně identifikoval spojení s neznámými IP adresami mimo univerzitní síť, což naznačovalo možný pokus o neautorizovaný vzdálený přístup. Tento typ detekce byl hodnocen jako velmi efektivní, zejména vzhledem k možnosti generovat okamžité upozornění na podezřelou komunikaci.

Omezení a nedostatky

Přestože modul Flowmon ADS prokázal svou schopnost detekovat široké spektrum hrozeb, během testování bylo identifikováno i několik slabých míst. Jedním z nich byla vyšší míra falešně pozitivních detekcí u některých metod, zejména při detekci DNS anomálií. Vzhledem k dynamické povaze univerzitní sítě, kde jsou často využívány různé experimentální servery a služby, bylo nutné opakovaně označovat falešné poplachy a přizpůsobovat detekční algoritmy. Na Obrázek 10 můžeme vidět že neobsahuje zatím žádná data o falešně pozitivních událostech.



Obrázek 10: Uživatelské rozhladní „False Positive“

(zdroj: vlastní)

Dalším problémem bylo zpracování velkého objemu tokových dat během špičkových časů. Přestože systém dokázal data analyzovat bez ztráty paketů, docházelo v některých případech ke zpomalení reakční doby při zobrazení výsledků v Monitoring Center. Tento jev byl pravděpodobně způsoben omezenými výpočetními prostředky virtuálního prostředí, ve kterém byl Flowmon ADS nasazen.

Celkové zhodnocení

Celkově lze funkčnost Flowmon ADS hodnotit pozitivně. Systém dokázal detekovat jak známé typy útoků (např. brute-force pokusy, DDoS útoky), tak i méně obvyklé typy anomálií (DNS Tunneling, RDP připojení k neznámým IP adresám). Modul se osvědčil zejména v oblasti detekce provozních anomálií, kde poskytl užitečné informace o komunikaci, která se odchylovala od běžného chování.

Důležitou roli sehrál i přehledný a dobře strukturovaný výstup, který umožňoval snadnou interpretaci výsledků a jejich následnou integraci do bezpečnostních politik univerzitní sítě. Přestože bylo třeba provést určité úpravy v nastavení detekčních metod, celková spolehlivost systému a jeho přínos pro bezpečnost sítě byly hodnoceny jako významné.

6 NÁVRHY NA ROZVOJ A ÚPRAVY FUNKCIONALIT NÁSTROJE FLOWMON

Nasazením systému Flowmon v prostředí univerzitní sítě Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně bylo dosaženo řady pozitivních výsledků, zejména v oblasti zabezpečení, provozní kontroly a optimalizace síťového provozu. Vzhledem k vysoké variabilitě typů zařízení, širokému spektru provozovaných služeb a dynamické struktuře provozu v univerzitních sítích, bylo rozhodnuto o nasazení řešení, které umožní efektivní monitoring a detekci hrozeb v reálném čase.

Pozitivní dopad byl zaznamenán zejména v oblasti detekce anomálního provozu a reakce na incidenty. Pomocí nástroje Flowmon ADS bylo zajištěno odhalování pokročilých typů hrozeb, včetně brute-force útoků na SSH, DNS tunnelingu a neobvyklých přenosů dat mimo pracovní dobu. Důraz byl kladen především na behaviorální analýzu a možnosti strojového učení, jejichž efektivita se prokázala právě v proměnlivém prostředí univerzitní sítě.

Efektivita jednotlivých modulů

Při testování byla zjišťována účinnost jednotlivých modulů systému Flowmon na základě jejich schopnosti detekovat incidenty, poskytovat provozní přehled a přispět ke zlepšení správy infrastruktury. Zaměření bylo směřováno na tři hlavní moduly – Flowmon Monitoring Center, Flowmon ADS a Flowmon DDoS Defender.

Modul Monitoring Center se osvědčil jako nejvšestrannější komponenta, jejímž prostřednictvím byl zajištěn nepřetržitý přehled o aktuálním provozu a následná detailní analýza. Zásadní výhodou bylo použití standardů NetFlow v9 a IPFIX, které umožnily detailní sledování datových toků bez potřeby instalace dodatečného hardware. Výsledky byly využívány k identifikaci přetížených segmentů, analýze vytížených VLAN a sledování kritických přenosových tras. Efektivita byla podpořena možností automatizovaného generování periodických reportů a jejich následné prezentace vedení fakulty.

Modul Flowmon ADS prokázal klíčový význam v oblasti detekce bezpečnostních incidentů. Detekce byla prováděna jak na základě porovnání se signaturami, tak především pomocí behaviorálních vzorců, což umožnilo odhalit i dosud neznámé typy hrozeb (tzv. zero-day útoky). Během testování byla využita funkce korelace s blacklisty (např. AbuseIPDB) a s tím spojená možnost včasného upozornění na komunikaci s nežádoucími IP adresami. Byla rovněž ověřena schopnost systému detekovat odchylky od standardního provozu

v různých VLAN segmentech a na základě toho automaticky vyhodnotit úroveň rizika incidentu.

Modul DDoS Defender byl využit především při simulaci volumetrických útoků. Jeho efektivita byla podpořena možností automatického přesměrování provozu do tzv. scrubbing center či zasílání mitigačních příkazů na firewall. Detekce nárůstu UDP/TCP paketů probíhala s minimálním zpožděním a systém byl schopen reagovat v řádu jednotek sekund. Důležitou funkcí byla možnost definování prahových hodnot provozu pro jednotlivé IP adresy, což umožnilo efektivní detekci i cílenějších útoků na konkrétní služby.

Z hlediska celkové efektivity se jako nejvýhodnější ukázala kombinace všech výše uvedených modulů, která poskytla vícevrstvou ochranu a zároveň umožnila jak retrospektivní analýzu incidentů, tak i jejich prediktivní sledování. Tento přístup by měl být i nadále zachován a dále rozvíjen, například integrací s externími nástroji pro správu incidentů (SIEM) nebo nasazením pokročilejších detekčních pravidel v rámci ADS.

Omezení zaznamenaná během testování

Přestože bylo nasazením systému Flowmon v akademickém prostředí dosaženo řady pozitivních výsledků, během testování byla identifikována i určitá funkční a provozní omezení. Tato omezení by měla být zohledněna při plánování dalšího nasazení a rozšiřování systému.

Za jedno z nejvýznamnějších omezení byla považována nutnost pravidelné optimalizace detekčních pravidel, zejména v modulu Flowmon ADS. Tento modul využívá behaviorální analýzu a průběžné učení na základě provozních vzorců, přičemž bylo zjištěno, že při každé významnější změně v infrastruktuře (např. přidání nového segmentu sítě, zavedení nového typu provozu nebo změna topologie VLAN) bylo nezbytné provést ruční aktualizaci detekčních parametrů. Pokud taková aktualizace nebyla provedena, docházelo k nárůstu falešných pozitiv, především při detekci komunikace na nezvyklých portech nebo při netypickém objemu přenesených dat. Doporučuje se proto zavedení mechanismu, kterým by byla detekce těchto změn automatizována a systém by byl schopen nabídnout úpravu modelů bez manuálního zásahu administrátora.

Dále byla zjištěna závislost systému na kvalitě a úplnosti tokových dat, exportovaných prostřednictvím protokolů NetFlow v9 a IPFIX. V několika případech byla detekce komplikována absencí informací z aplikační vrstvy. Tato situace se projevila zejména při šifrované komunikaci, kde nebylo možné využít inspekci obsahu. Byla navržena možnost

doplnění metadat pomocí integrace s nástroji typu TLS fingerprinting (např. JA3), jejichž nasazení by mohlo zpřesnit identifikaci podezřelých spojení, aniž by bylo nutné narušovat soukromí komunikace.

Dalším omezením byl omezený rozsah přednastavených detekčních scénářů, které nebyly vždy plně přizpůsobeny specifickým požadavkům akademického prostředí. Detekce brute-force útoků a skenování portů byla sice technicky možná, avšak bez ruční konfigurace citlivosti detekce nebylo dosaženo potřebné přesnosti. Doporučuje se proto vytvořit šablony scénářů přímo pro vysokoškolské sítě, včetně možnosti importu přednastavených prahových hodnot dle charakteru provozu.

Z pohledu technického provozu se jako omezení ukázalo zatížení systému během provozních špiček. V období, kdy byly prováděny například aktualizace softwaru nebo masivní zálohování, docházelo ke zpomalení odezvy uživatelského rozhraní. Bylo zjištěno, že toto zpomalení bylo způsobeno limitem výkonu diskového pole a nedostatečnou optimalizací archivace tokových dat. Jako řešení se doporučuje zavedení plánované rotace a archivace na externí úložiště a případné využití SSD pro provozní část databáze.

Jako poslední bylo zaznamenáno omezené využití integračních možností systému Flowmon s dalšími bezpečnostními nástroji. Ačkoli je k dispozici podpora protokolů jako Syslog a API konektory, v praxi nebylo z důvodu technických omezení infrastruktury realizováno napojení na nástroje typu vulnerability scanner či komplexní SIEM systémy. Bylo navrženo, aby byla v budoucnu vypracována konkrétní integrační strategie, která by zahrnovala postup propojení Flowmonu například s nástroji jako Nessus, Splunk nebo Graylog.

Z výše uvedených skutečností vyplývá, že ačkoliv nebyla provozuschopnost systému Flowmon výrazně omezena, některé oblasti vyžadují systematický dohled, pravidelnou revizi nastavení a technické úpravy infrastruktury. V následující kapitole budou tato zjištění promítnuta do návrhů na rozvoj a konkrétní kroky směřující ke zvýšení spolehlivosti a přehlednosti systému v akademickém prostředí. Souhrn zjištěných omezení lze vidět v

Tabulka 9: Přehled zjištěných omezení

Identifikované omezení	Popis problému	Doporučené řešení
Nutnost ruční údržby detekčních pravidel	Vyšší počet falešných pozitiv při změnách sítě	Zavést automatické přizpůsobení modelů
Nedostatečné informace v tokových datech	Absence dat z aplikační vrstvy u šifrovaného provozu	Využití TLS fingerprintingu (např. JA3)
Omezený rozsah detekčních scénářů	Detekce útoků závislá na správně nastavených hodnotách	Tvorba přednastavených scénářů pro univerzitní síť
Výkonové limity při provozní špičce	Zpomalení odezvy systému	Optimalizace archivace, využití SSD
Nedostatečná integrace s dalšími nástroji	Chybějící napojení na SIEM nebo vulnerability scanning	Vypracování konkrétní integrační strategie

(zdroj: vlastní)

Uživatelská zkušenost a přístupnost systému

Uživatelská zkušenost s nasazením systému Flowmon v univerzitní síti byla celkově pozitivní, a to jak z hlediska přístupnosti rozhraní, tak z hlediska jeho přehlednosti a možností přizpůsobení konkrétním potřebám. Systém Flowmon poskytoval jednotné webové rozhraní, které bylo přístupné prostřednictvím zabezpečeného protokolu HTTPS. Tento způsob přístupu umožňoval snadnou správu jak z interní sítě, tak v případě potřeby i z externího prostředí při využití VPN.

Z hlediska uživatelského rozhraní byla hodnocena především přehlednost a intuitivnost systému. Administrátoři oceňovali jasnou strukturu hlavního menu, které bylo rozděleno na jednotlivé moduly (Monitoring Center, ADS, DDoS Defender atd.), přičemž každý modul měl své vlastní specializované nástroje pro zpracování a analýzu dat. Navigace mezi

jednotlivými částmi systému byla plynulá a uživatelé měli možnost rychlého přístupu k relevantním informacím bez zbytečného proklikávání.

Pozitivně byla hodnocena také možnost přizpůsobení dashboardů a přehledů. Systém umožňoval tvorbu vlastních pohledů, které mohly být nastaveny podle potřeb konkrétního administrátora. Uživatelé mohli vytvářet přehledy zaměřené na sledování konkrétních VLAN, protokolů nebo síťových událostí, což značně zjednodušovalo práci při monitorování specifických problémů nebo sledování bezpečnostních incidentů.

Z pohledu přístupnosti bylo rozhraní Flowmon hodnoceno jako dostatečně robustní i při práci s většími objemy dat. Například při zpracování toků za posledních 30 dní nebo při porovnávání statistik z více VLAN nedocházelo k výraznému zpomalení systému. To bylo možné především díky efektivnímu využívání předindexovaných databází a optimalizovanému způsobu ukládání tokových dat.

Jistá omezení však byla zaznamenána u uživatelů bez pokročilých znalostí v oblasti síťové bezpečnosti a analýzy dat. Přestože byl systém navržen s důrazem na přehlednost, některé pokročilé funkce (např. tvorba komplexních filtrů nebo práce s heuristickými metodami v ADS) vyžadovaly určitou odbornou znalost. Bez předchozího školení nebo prostudování dokumentace mohlo dojít k nesprávnému vyhodnocení výsledků nebo přehlédnutí důležitých informací.

Dalším aspektem, který byl v rámci uživatelské zkušenosti zmiňován, byla nutnost pravidelné údržby a aktualizace systému. Především u modulu ADS bylo třeba pravidelně kontrolovat nastavení detekčních metod, aby se minimalizovaly falešné poplachy a zároveň nedocházelo k přehlížení skutečných bezpečnostních incidentů. Někteří administrátoři uváděli, že by uvítali automatizovanější způsob aktualizace modelů chování a širší možnosti integrace se SIEM systémy pro jednotnou správu událostí.

Celkově však byl Flowmon hodnocen jako velmi přístupný nástroj pro běžné monitorování sítě a zároveň jako efektivní řešení pro pokročilé bezpečnostní analýzy. Uživatelské rozhraní bylo navrženo s důrazem na jednoduchost a přehlednost, přičemž jeho možnosti lze rozšiřovat podle potřeb konkrétní organizace. Díky této flexibilitě bylo možné systém efektivně nasadit i v akademickém prostředí, kde je požadována jak schopnost detailní analýzy, tak jednoduchá administrace.

Celkové shrnutí a identifikace prostoru pro rozvoj

Celkové hodnocení systému Flowmon v prostředí univerzitní sítě Fakulty krizového řízení a logistiky Univerzity Tomáše Bati ukazuje, že nasazení tohoto nástroje přineslo výrazné zlepšení v oblasti monitorování síťového provozu, detekce anomálií a reakce na bezpečnostní incidenty. Díky kombinaci modulů Monitoring Center, ADS a DDoS Defender se podařilo vytvořit efektivní bezpečnostní ekosystém, který poskytuje komplexní přehled o dění v síti a umožňuje rychlé reakce na podezřelé aktivity.

Významným přínosem bylo nasazení modulu Monitoring Center, který umožnil detailní analýzu provozu na úrovni síťových toků. Administrátoři ocenili možnost sledovat provoz nejen na aplikační vrstvě, ale také na úrovni protokolů, portů a VLAN. Přehledy zaměřené na nejvytíženější zařízení, komunikační vztahy a typy používaných služeb poskytly cenné informace pro optimalizaci infrastruktury i řešení provozních problémů.

Modul Flowmon ADS rovněž prokázal svou efektivitu při detekci bezpečnostních incidentů a anomálií. Díky využití metod behaviorální analýzy a heuristických pravidel bylo možné identifikovat incidenty, které by byly u tradičních signaturních systémů přehlédnuty. ADS dokázal odhalit nejen známé útoky, ale také neobvyklé vzorce chování, které mohly souviset s dosud neznámými hrozbami. Možnost zpětného vyhodnocování incidentů byla klíčová při forenzní analýze a při zlepšování detekčních pravidel.

Některá omezení byla zaznamenána v oblasti uživatelské přístupnosti a potřeby pokročilých znalostí při konfiguraci detekčních metod v modulu ADS. Přestože základní monitoring byl intuitivní a snadno přístupný, práce s pokročilými detekčními metodami vyžadovala hlubší znalosti z oblasti síťové bezpečnosti. To představovalo určitou překážku zejména pro méně zkušené administrátory.

Dalším slabším místem bylo omezení systému při detekci útoků zaměřených na šifrovaný provoz. Ačkoliv byly dostupné metody jako TLS fingerprinting, absence možnosti hluboké inspekce paketů znemožňovala detekci útoků, které se skrývají uvnitř šifrovaného spojení. Tento problém je obecný pro všechny systémy založené na tokové analýze, přesto by jeho řešení mohlo představovat zásadní krok kupředu.

Prostor pro rozvoj

Přes výše uvedená omezení byl systém Flowmon hodnocen jako efektivní nástroj pro zabezpečení a správu univerzitní sítě. Pro další zvýšení účinnosti a uživatelské přívětivosti jsou navrhovány následující kroky:

Zlepšení integrace s externími bezpečnostními nástroji – Rozšíření možností propojení se SIEM systémy, jako je Splunk, Graylog nebo IBM QRadar, by umožnilo efektivnější korelaci událostí a centralizovanou správu incidentů.

Rozšíření podpory pro detekci šifrovaného provozu – Zavedení pokročilejších metod pro analýzu TLS komunikace (např. JA3 fingerprinting, analýza SNI) a rozšíření heuristických pravidel pro detekci škodlivého provozu skrytého uvnitř šifrovaných přenosů.

Uživatelsky přívětivější rozhraní pro práci s ADS – Zjednodušení konfigurace detekčních metod, především možnost automatizovaného učení bez nutnosti manuálního zásahu administrátora. Tento krok by mohl výrazně snížit počet falešných poplachů a zároveň zvýšit přesnost detekce.

Zlepšení podpory pro cloudová a hybridní prostředí – Rozšíření možnosti monitorování v prostředí, kde dochází ke komunikaci mezi on-premise infrastrukturou a cloudovými službami, by poskytlo komplexnější pohled na síťovou bezpečnost.

Zpřesnění notifikací a reportování – Přidání možností pro personalizované reporty a notifikace by umožnilo administrátorům přizpůsobit systém konkrétním potřebám a zvýšit efektivitu při správě bezpečnostních incidentů.

Závěrem lze konstatovat, že Flowmon se ukázal jako vhodný nástroj pro správu a zabezpečení univerzitní sítě, který nabízí široké spektrum funkcí jak pro provozní monitoring, tak pro detekci bezpečnostních incidentů. Implementace navržených vylepšení by mohla dále zvýšit efektivitu systému a přispět k dosažení vyšší úrovně bezpečnosti.

6.1 Možnosti rozšíření funkcionality

Automatizace reakce na bezpečnostní incidenty se v současnosti stává jedním z klíčových prvků moderního zabezpečení sítí. Cílem tohoto přístupu je snížit dobu potřebnou k identifikaci a odstranění hrozeb, minimalizovat riziko lidské chyby a umožnit bezpečnostním týmům soustředit se na složitější problémy, které vyžadují jejich odborné znalosti. Flowmon díky své architektuře a integraci s dalšími bezpečnostními nástroji umožňuje do značné míry automatizovat reakci na detekované incidenty.

Modul Flowmon ADS poskytuje několik možností automatizované reakce, které mohou být nakonfigurovány na základě detekovaných anomálií či podezřelých aktivit.

Mezi hlavní metody automatizované reakce patří:

Generování výstrah a notifikací

Pokud dojde k detekci události, která překračuje nastavené prahové hodnoty, systém automaticky odesílá upozornění prostřednictvím e-mailu, Syslogu nebo webhooku. Tato notifikace může být předána jak přímo administrátorům, tak i externím systémům, například SIEM platformám typu IBM QRadar nebo Splunk. Výstrahy jsou důležitým prvkem automatizace, protože umožňují okamžité upozornění na kritické události bez nutnosti manuální kontroly rozhraní Flowmonu.

Blokování provozu prostřednictvím firewallu

V případě detekce kritického incidentu, jako je například pokus o průnik nebo komunikace s C&C servery, může být Flowmon nakonfigurován tak, aby zaslal příkaz k firewallu nebo IDS/IPS systému pro okamžité zablokování konkrétní IP adresy nebo portu. Tato funkce byla v testovaném prostředí využita například při detekci škodlivých DNS dotazů, kdy byl přístup zařízení na nebezpečné adresy automaticky blokován.

Integrace s dalšími bezpečnostními nástroji

Flowmon podporuje standardní protokoly a API rozhraní, která umožňují propojení s dalšími bezpečnostními systémy. Typicky se jedná o systémy typu SIEM, kde mohou být zaznamenané incidenty korelovány s dalšími daty z infrastruktury a poskytovat tak širší kontext. V testovaném prostředí nebyla plná integrace s externím SIEM systémem realizována, ale možnost propojení byla ověřena pomocí Syslog exportů.

Aktivní mitigace DDoS útoků

Modul Flowmon DDoS Defender umožňuje detekci volumetrických útoků a automatickou spolupráci se scrubbing centry nebo firewally. Jakmile je útok detekován, systém může automaticky přesměrovat provoz do externího centra na očištění od škodlivého provozu, čímž se zabrání přetížení infrastruktury. Tato metoda byla v testovaném prostředí úspěšně otestována při simulaci DDoS útoku na univerzitní síť.

Adaptivní učení a vylepšování detekčních pravidel

Flowmon ADS umožňuje uživateli označovat incidenty jako „false positive“ nebo potvrzovat jejich skutečnou relevanci. Tento způsob učení přispívá k neustálému zlepšování detekčního modelu a umožňuje systému lépe se přizpůsobit specifickému prostředí univerzitní sítě.

Implementace automatizované reakce přinesla v testovaném prostředí významné zlepšení v oblasti rychlosti reakce na incidenty a minimalizace jejich dopadu. Automatizace umožnila eliminovat některé typy útoků ještě předtím, než mohly způsobit škody, což bylo prokázáno například při testování reakce na DDoS útoky. Zároveň se snížil počet falešných poplachů, protože systém byl schopen se adaptovat na konkrétní provozní charakteristiky univerzitní sítě.

Nicméně bylo také zjištěno, že plné využití možností automatizované reakce vyžaduje podrobné nastavení detekčních metod a pravidel. Nedostatečně konfigurované filtry mohou vést buď k vysokému počtu falešných pozitiv, nebo naopak k přehlížení relevantních incidentů. Toto riziko je možné snížit pravidelným hodnocením a optimalizací nastavení.

Z hlediska dalšího rozvoje by bylo vhodné zlepšit možnosti integrace s externími systémy a rozšířit škálu možných automatických reakcí. V prostředí univerzitní sítě by bylo přínosné zejména zapojení automatizovaných postupů pro blokaci nežádoucích IP adres nebo komunikace s rizikovými doménami. To by umožnilo dosáhnout vyšší úrovně ochrany při zachování minimální zátěže na lidské zdroje.

Rozšíření podpory aplikačních protokolů (L7)

V rámci rozvoje systému Flowmon se ukazuje jako klíčové rozšíření podpory aplikačních protokolů (L7), které představují nejvyšší vrstvu v modelu OSI a zahrnují konkrétní aplikace a služby, jako jsou DNS, HTTP, HTTPS, SMTP, FTP, či VoIP. Zatímco základní toková analýza je založena především na údajích z nižších vrstev, pokročilá analýza aplikační vrstvy umožňuje přesnější detekci hrozeb, optimalizaci provozu a lepší přehled o síťových aktivitách.

V testovaném prostředí bylo zjištěno, že Flowmon umožňuje rozšířený sběr metadat z aplikační vrstvy pomocí protokolů NetFlow v9 a IPFIX, které podporují rozšíření o L7 informace. Konkrétně se jedná například o podporu HTTP hlaviček, DNS dotazů

a odpovědí, identifikaci TLS handshake včetně fingerprintingu (JA3) a analýzu specifických služeb jako je SMB, NTP či DHCP.

Jednou z hlavních výhod této funkce je schopnost detailně sledovat šifrovaný provoz bez nutnosti dešifrování obsahu. Flowmon využívá TLS fingerprinting (JA3), což je technika založená na vytváření otisků (hashů) z handshake zpráv v rámci TLS komunikace. Tento otisk umožňuje identifikovat konkrétní aplikace či verze klientů, aniž by bylo nutné dekódovat samotnou šifrovanou komunikaci. V testovaném prostředí byla tato metoda využita k odhalení nestandardního provozu na portech TCP/443 a TCP/8443, kde byly zachyceny neobvyklé TLS fingerprinty odpovídající neznámým nebo podezřelým aplikacím.

Podpora L7 analýzy se ukázala jako klíčová při sledování provozu v bezdrátové síti, kde byl identifikován zvýšený počet DNS dotazů na neexistující nebo podezřelé domény. Modul Flowmon ADS byl schopen tyto dotazy identifikovat a klasifikovat je jako potenciální tunneling nebo C&C komunikaci. Tento typ analýzy je důležitý zejména v prostředí, kde je častý přístup uživatelů ke vzdáleným službám a kde by standardní L3/L4 analýza nebyla schopna detekovat jemnější odchylky od běžného provozu.

V rámci aplikace rozšířené L7 podpory bylo možné sledovat i protokoly jako SMB nebo RDP, které byly využívány pro vzdálenou správu a sdílení souborů. Tato detekce přispěla k identifikaci případů, kdy některá zařízení neoprávněně přistupovala ke sdíleným složkám nebo se pokoušela o vzdálený přístup mimo běžnou pracovní dobu. Díky tomu bylo možné upravit přístupová pravidla a zvýšit zabezpečení těchto služeb.

V oblasti rozšíření podpory L7 je důležité zmínit i možnost integrace Flowmonu s dalšími nástroji, které se specializují na analýzu konkrétních protokolů nebo aplikací. Tato integrace je realizována prostřednictvím API rozhraní nebo exportů dat do SIEM systémů, kde mohou být další detekce nebo korelace prováděny na základě specifických pravidel nebo signatur.

Hlavní přínosy rozšíření podpory L7 v testovaném prostředí zahrnují:

- Detailní analýzu šifrované komunikace bez nutnosti dešifrování (např. pomocí TLS fingerprintingu).
- Možnost sledování specifických aplikačních protokolů (DNS, HTTP, SMB, RDP).
- Lepší detekci neobvyklého provozu nebo zneužívání služeb (např. DNS tunneling, neautorizované sdílení souborů).

- Přesnější klasifikaci provozu a tvorbu politik pro bezpečnostní detekce.

Nicméně bylo zjištěno, že rozšířená podpora aplikačních protokolů vyžaduje důkladné nastavení detekčních pravidel a pravidelnou aktualizaci fingerprintů a signatur. V testovaném prostředí byla například zjištěna vyšší míra falešných pozitiv při detekci HTTP provozu, což bylo způsobeno neúplným mapováním použitých aplikací. Tento problém lze řešit přizpůsobením pravidel pro konkrétní prostředí a průběžným sledováním vývoje nových protokolů a jejich verzí.

Rozšíření podpory aplikačních protokolů v rámci systému Flowmon představuje významný krok směrem k vyšší přesnosti detekce hrozeb a lepší viditelnosti síťového provozu. Do budoucna by bylo vhodné tuto funkcionalitu rozvíjet zejména směrem k hlubší integraci s ostatními bezpečnostními nástroji a k podpoře nově vznikajících protokolů a technologií.

Pokročilé detekční scénáře a pravidla

Systém Flowmon ADS umožňuje vytváření pokročilých detekčních scénářů a pravidel, které výrazně rozšiřují schopnost detekce bezpečnostních incidentů a anomálií v síťovém provozu. Zatímco základní detekční pravidla jsou předdefinována a zahrnují detekci běžných typů útoků či nestandardního chování, pokročilé scénáře umožňují uživateli konfigurovat vlastní pravidla šitá na míru konkrétním potřebám sítě. Tento přístup je nezbytný zejména v heterogenním prostředí, jakým je univerzitní síť s různými typy provozu a rozdílnými požadavky na bezpečnost.

Pokročilá pravidla jsou v systému Flowmon ADS vytvářena na základě kombinace několika metod detekce, jako jsou heuristická analýza, behaviorální modelování, porovnávání se signaturami a korelace s externími blacklisty. Administrátor má možnost využít různé kombinace těchto metod k vytvoření vlastních scénářů detekce.

Jedním z příkladů pokročilého detekčního scénáře v testovaném prostředí bylo sledování komunikace na nezvyklých portech nebo použití netypických protokolů v určitých VLAN. Například v síti určené pro studenty byl definován scénář, který sledoval provoz na portech vyšších než 50 000, což mohlo indikovat použití nástrojů pro proxy tunneling nebo neautorizovanou P2P komunikaci. Bylo zjištěno, že opakované pokusy o přístup na neznámé porty se shodovaly s obdobím, kdy studenti využívali vzdálené přístupy k testování vlastních aplikací.

Další využitý scénář se zaměřoval na detekci dlouhodobých spojení, která neodpovídala běžnému provozu. Běžná komunikace mezi servery a pracovními stanicemi má typicky krátkodobý charakter, přičemž dlouhotrvající spojení mohou indikovat snahy o přenos velkých objemů dat nebo pokusy o udržení otevřeného připojení s externími servery. Flowmon ADS umožňuje nastavit pravidla pro identifikaci takových spojení na základě délky trvání komunikace, počtu přenesených paketů či objemu přenesených dat.

Vzhledem k narůstajícímu množství šifrovaného provozu bylo rovněž zavedeno pravidlo pro sledování nestandardních TLS fingerprintů (JA3). Pomocí této metody bylo možné identifikovat specifické aplikace či klienty, které komunikovaly na portech typických pro HTTPS, ale používaly neobvyklé TLS fingerprinty. Tento typ pravidla je zvláště důležitý pro detekci malware komunikace nebo nestandardních VPN nástrojů, které se snaží obejít bezpečnostní politiky sítě.

Pokročilé detekční scénáře mohou být rovněž založeny na sledování komunikace s externími IP adresami, které jsou uvedeny na blacklistu. Flowmon ADS podporuje import blacklistů jak z veřejných zdrojů (např. Spamhaus, AbuseIPDB), tak z vlastních seznamů spravovaných administrátory. V testovaném prostředí byly použity zejména blacklisty zaměřené na identifikaci botnetů a C&C serverů. Detekce komunikace s takovými IP adresami byla okamžitě označována jako kritická a předávána ke korekci.

Kromě statických blacklistů byl využit i přístup založený na korelaci mezi různými typy provozu. Například detekce opakovaných DNS dotazů směřovaných na neznámé domény byla kombinována s analýzou komunikace přes porty typické pro škodlivé aplikace (např. TCP/6667 – IRC, TCP/12345 – NetBus). Tato kombinace umožnila detekci podezřelých aktivit, které by samostatně nebyly dostatečně závažné pro vyvolání alarmu.

Vytváření a správa pokročilých detekčních pravidel je v systému Flowmon ADS realizována prostřednictvím přehledného webového rozhraní, kde lze nastavit citlivost pravidel, definovat výjimky a sledovat historii detekcí. V rámci testování bylo ověřeno, že jednotlivá pravidla mohou být vytvářena ručně nebo na základě doporučení generovaných Flowmon ADS. Tento přístup umožňuje kontinuální adaptaci systému na nové hrozby a poskytuje administrátorům možnost přesně definovat, které typy provozu mají být považovány za podezřelé.

Výsledky detekcí jsou zobrazeny v rámci přehledů v modulu Monitoring Center, kde je možné provádět detailní analýzu a sledovat dlouhodobé trendy. Flowmon ADS nabízí také

možnost automatického generování reportů nebo zasílání upozornění na detekované incidenty prostřednictvím e-mailu či Syslogu. Tyto možnosti zajišťují rychlou reakci na bezpečnostní události a poskytují komplexní přehled o stavu síťové bezpečnosti.

Nasazení pokročilých detekčních pravidel se ukázalo jako velmi efektivní nástroj pro identifikaci potenciálních hrozeb, které by nebyly zachyceny pomocí základních metod. Další rozvoj této oblasti by měl směřovat ke zlepšení integrace Flowmon ADS s jinými bezpečnostními nástroji a ke zpřesňování heuristických modelů pro detekci nově vznikajících typů útoků.

Rozšíření možností vizualizace a dashboardů

V rámci testovaného prostředí se modul Flowmon Monitoring Center ukázal jako efektivní nástroj pro vizualizaci síťového provozu a prezentaci klíčových statistik v přehledných dashboardech. Nicméně, jednou z hlavních oblastí pro budoucí rozvoj systému je rozšíření možností vizualizace a tvorby vlastních dashboardů, které by umožnily uživatelům snadněji přizpůsobit výstupy jejich specifickým potřebám a zároveň zlepšit přehlednost a dostupnost důležitých informací.

V současné době Flowmon Monitoring Center poskytuje širokou škálu předdefinovaných přehledů a grafů, zahrnujících například Top Hosts, Top Conversations, Top Protocols a Top VLANs. Tyto přehledy jsou zobrazovány ve formě časových grafů, sloupcových diagramů, tabulek a heatmap. Uživatelé mohou vybírat časová období, aplikovat filtry a nastavovat různé úrovně detailů, což poskytuje dostatečný základ pro standardní analytické činnosti.

Přesto se ukázalo, že stávající možnosti vizualizace by mohly být dále rozšířeny o následující funkce:

Tvorba vlastních grafů a metrik: Uživatelé by měli mít možnost vytvářet zcela nové typy grafů, které by kombinovaly různé metriky do jednoho přehledu. Například současné zobrazení objemu přenesených dat, počtu toků a počtu unikátních IP adres v jednom grafu by mohlo poskytnout ucelenější pohled na provoz v síti.

Dynamické a interaktivní dashboardy: Dashboardy v současné verzi systému jsou relativně statické. Možnost vytváření interaktivních přehledů, kde by uživatel mohl dynamicky přepínat mezi různými filtry nebo měnit časové rozsahy přímo v grafu, by významně zvýšila efektivitu práce. Rovněž by bylo přínosné umožnit tvorbu víceúrovňových dashboardů s možností drill-down analýzy.

Podpora dalších grafických typů: Vedle klasických časových grafů a tabulek by bylo vhodné rozšířit vizualizační možnosti o síťové mapy, diagramy vztahů či grafy topologie sítě. Tato funkcionalita by umožnila uživatelům lépe porozumět komunikaci mezi zařízeními, identifikovat kritická místa sítě nebo vizuálně sledovat průběh útoků.

Tvorba vlastních dashboardů: Ačkoliv systém Flowmon umožňuje určitou míru přizpůsobení dashboardů, uživatelé nejsou schopni plně definovat strukturu a obsah podle vlastních potřeb. Možnost tvorby uživatelských dashboardů na míru by významně zvýšila přehlednost zejména ve složitějších prostředích s vysokým objemem provozu nebo různorodými bezpečnostními požadavky.

Integrace s externími vizualizačními nástroji: Některé organizace využívají specializované platformy jako Grafana nebo Kibana pro vizualizaci dat. Umožnění exportu tokových dat do těchto nástrojů v reálném čase by umožnilo tvorbu komplexních přehledů a jejich integraci do širšího bezpečnostního ekosystému.

Notifikace a alerty v dashboardech: Systém Flowmon umožňuje zasílání upozornění na detekované incidenty prostřednictvím e-mailu nebo Syslogu. Nicméně, možnost vizuálního zobrazení těchto alertů přímo v dashboardu by poskytla administrátorům rychlejší přístup k důležitým informacím a usnadnila jejich vyhodnocování.

Prediktivní analýza a zobrazení trendů: Implementace prediktivních algoritmů by umožnila vytvářet přehledy zaměřené na předvídaní potenciálních problémů na základě dosavadních trendů. Například zvýšený počet DNS dotazů nebo nestandardní růst komunikace na určitém portu by mohl být vizuálně zobrazen jako varovný indikátor.

Rozšíření možností vizualizace by přineslo zlepšení nejen pro bezpečnostní monitoring, ale také pro optimalizaci síťového provozu a správu infrastruktury. Flowmon by se tímto krokem mohl přiblížit k řešení typu SIEM (Security Information and Event Management), která poskytují široké možnosti analytiky a zobrazení dat z různých zdrojů.

Vzhledem k tomu, že současné trendy v oblasti kybernetické bezpečnosti kladou důraz na integraci a unifikaci analytických nástrojů, bylo by vhodné, aby systém Flowmon pokračoval v rozšiřování svých možností nejen v oblasti detekce, ale i prezentace a vizualizace informací.

Automatizovaný reporting

Automatizovaný reporting představuje důležitou funkci nástroje Flowmon, která umožňuje pravidelnou a systematickou tvorbu přehledů o síťovém provozu, detekovaných anomáliích a bezpečnostních incidentech. Tato funkcionalita je nezbytná především v prostředích, kde je požadována transparentnost síťových aktivit, dokumentace bezpečnostních událostí a zpětná analýza komunikace. Automatizovaný reporting také usnadňuje komunikaci mezi administrátory a managementem, neboť poskytuje srozumitelně strukturované výstupy v pravidelných intervalech.

V systému Flowmon lze reporty generovat buď manuálně na požádání, nebo zcela automatizovaně na základě předem definovaných plánů. Tento proces umožňuje vytvořit ucelený pohled na síťový provoz a jeho chování za uplynulé období, což je klíčové pro dlouhodobé sledování trendů, optimalizaci síťové infrastruktury a kontrolu dodržování bezpečnostních politik.

Vlastnosti a výhody automatizovaného reportingu

Automatizovaný reporting v prostředí Flowmon zahrnuje následující klíčové funkce:

Periodické reporty: Reporty mohou být generovány denně, týdně, měsíčně nebo v jiném uživatelem definovaném intervalu. Tato možnost je výhodná zejména pro pravidelné sledování výkonu sítě, detekce anomálií a analýzu výkonnostních metrik.

Přizpůsobitelné šablony: Flowmon umožňuje vytvářet vlastní šablony pro reporty, které zahrnují pouze relevantní metriky a přehledy. Uživatel může nastavit, jaké grafy, tabulky nebo textové výstupy budou součástí každého reportu. Tato flexibilita zajišťuje, že reporty jsou vždy přizpůsobeny konkrétním potřebám organizace.

Formáty výstupů: Reporty lze exportovat ve formátech PDF, CSV, JSON nebo XML, což umožňuje jejich snadnou archivaci nebo integraci s dalšími analytickými nástroji. Výstupy mohou být rovněž prezentovány ve formě grafů, tabulek nebo časových os, což přispívá k lepší přehlednosti a interpretaci dat.

Distribuce reportů: Automatizované reporty mohou být zasílány e-mailem vybraným příjemcům, což zajišťuje, že se klíčové informace dostanou k odpovědným osobám bez nutnosti manuálního přístupu do systému Flowmon. Tato funkce je cenná zejména při předávání informací mezi různými týmy či odděleními.

Notifikace o vytvoření reportu: Kromě přímé distribuce může systém zasílat upozornění na vytvoření reportu prostřednictvím e-mailu nebo Syslog zpráv. Tím je zajištěno, že administrátor je informován o dokončení procesu generování reportu i v případě, že se do systému Flowmon nepřihlásí.

Korelace s bezpečnostními událostmi: Díky integraci s modulem Flowmon ADS mohou být reporty automaticky generovány i na základě detekovaných incidentů. Například v případě, že je zaznamenána podezřelá komunikace, může systém ihned vytvořit detailní report obsahující všechny relevantní informace o daném jevu.

Archivace a zpětné vyhodnocení: Uložené reporty mohou být využity pro zpětnou analýzu provozu nebo porovnání s dřívějšími obdobími. Tento aspekt je zvláště cenný při řešení incidentů nebo při kontrole dlouhodobých trendů v síti.

Doporučení pro zlepšení automatizovaného reportingu

Přestože současná implementace automatizovaného reportingu v nástroji Flowmon poskytuje široké možnosti, několik oblastí by mohlo být v budoucnu dále rozvinuto:

Rozšíření možností přizpůsobení: Umožnit ještě detailnější nastavení struktury reportů, například dynamické vytváření přehledů na základě aktuálních dat nebo automatické porovnávání s minulými obdobími.

Vizualizace trendů: Implementovat prediktivní algoritmy, které by do reportů zahrnovaly i projekce budoucího vývoje na základě dosavadních dat.

Integrace s externími nástroji: Možnost přímého exportu reportů do cloudových aplikací nebo analytických platforem typu Grafana nebo Power BI, které jsou již v některých prostředích používány.

Automatizovaný reporting v systému Flowmon představuje klíčovou funkcionalitu, která výrazně usnadňuje dohled nad síťovým provozem a poskytuje cenné informace pro jeho optimalizaci a zabezpečení. V budoucnu by mohlo být prospěšné tuto funkcionalitu dále rozšířit, aby byla ještě lépe přizpůsobena specifickým potřebám akademického prostředí.

6.2 Vylepšení uživatelského rozhraní a přístupnosti systému

Jednou z klíčových vlastností systému Flowmon je jeho schopnost přizpůsobit se různým typům uživatelů prostřednictvím definovaných uživatelských rolí a přístupových práv. Tento přístup je zásadní zejména v akademickém prostředí, kde se správa sítě často dělí mezi

více oddělení nebo skupin uživatelů s různými potřebami a odpovědnostmi. Přístupnost systému pro různé role uživatelů nejen zvyšuje bezpečnost, ale také umožňuje efektivnější správu celého monitorovacího řešení.

Systém Flowmon nabízí robustní správu uživatelů prostřednictvím role-based access control (RBAC). Administrátor systému může vytvářet uživatelské účty s různými úrovněmi oprávnění, což umožňuje přesně definovat, jaké funkce a data jsou pro konkrétního uživatele dostupné. Tento přístup je důležitý zejména z hlediska bezpečnosti, protože umožňuje omezit přístup k citlivým informacím nebo konfiguracím pouze na pověřené osoby.

Typy uživatelských rolí

V systému Flowmon lze definovat různé role uživatelů podle jejich odpovědností a potřeb. Mezi nejčastěji využívané patří:

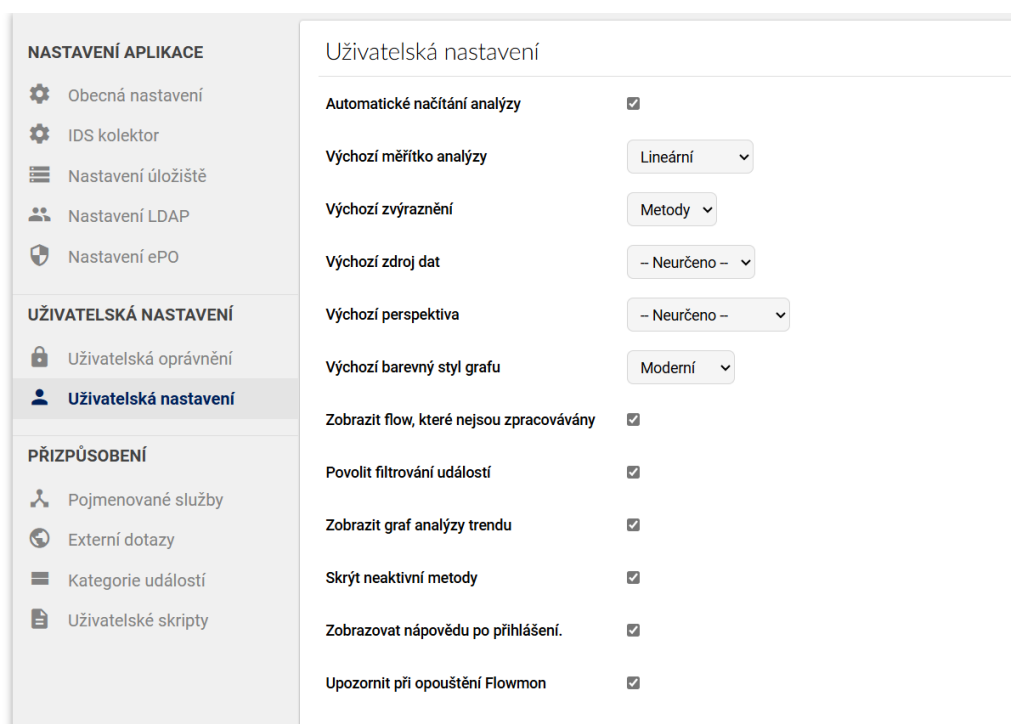
- **Administrátor (Full Access):** Administrátor má plný přístup ke všem funkcím systému, včetně konfigurace senzorů, nastavení modulů ADS a Monitoring Center, správy uživatelů a exportů dat. Tento typ uživatele je zpravidla odpovědný za kompletní správu monitorovacího řešení.
- **Analytik (Read-Only Access):** Analytik má přístup pouze k vizualizacím, přehledům a reportům, které jsou k dispozici v modulu Monitoring Center. Nemůže však měnit konfiguraci systému nebo nastavovat nové detekční metody. Tato role je ideální pro pracovníky, kteří se zabývají provozní analýzou a vyhodnocováním statistik bez přímého zásahu do konfigurace systému.
- **Bezpečnostní specialista (Security Analyst):** Uživatel s touto rolí má přístup k detekčním funkcím modulu ADS, kde může nastavovat pravidla, analyzovat incidenty a označovat falešně pozitivní detekce. Tento typ uživatele se zaměřuje na bezpečnostní aspekty provozu a zpravidla komunikuje s administrátory při řešení konkrétních incidentů.
- **Uživatel s omezeným přístupem (Restricted User):** Tato role je vhodná pro osoby, které potřebují přístup pouze ke konkrétnímu segmentu sítě nebo k předdefinovaným reportům. Například vedoucí pracovníci mohou mít přístup pouze k automatizovaným týdenním přehledům bez možnosti jejich úpravy.

- **Host (Guest):** Hostovský účet slouží pro dočasný přístup k systému, například při auditech nebo externích kontrolách. Tento typ uživatele má pouze omezené čtecí práva bez možnosti modifikace konfigurace nebo vytváření exportů.

Přizpůsobitelnost rozhraní

Pro každou roli lze v systému Flowmon nakonfigurovat vlastní uživatelské rozhraní s přístupem pouze k relevantním modulům a funkcím, jak lze vidět na Obrázek 11. To umožňuje nejen lepší přehlednost pro koncové uživatele, ale také zvyšuje bezpečnost tím, že eliminuje možnost neautorizovaných změn konfigurace.

Například analytici zaměření na provozní monitorování mají přístup pouze k modulu Monitoring Center, zatímco bezpečnostní specialisté pracují především s modulem ADS. Administrátor pak může spravovat kompletní konfiguraci a přidávat nebo odebírat uživatelské účty dle potřeby.



Obrázek 11: Uživatelské rozhraní

(zdroj: vlastní)

Výhody role-based access control (RBAC)

Implementace RBAC v systému Flowmon přináší několik významných výhod:

- **Bezpečnost:** Omezení přístupu ke kritickým funkcím pouze na autorizované uživatele minimalizuje riziko nechtěných nebo škodlivých zásahů do systému.
- **Efektivita:** Uživatelé mají přístup pouze k těm funkcím, které potřebují ke své práci, což zvyšuje přehlednost rozhraní a zjednodušuje správu systému.
- **Auditovatelnost:** Systém umožňuje sledovat a logovat aktivity jednotlivých uživatelů, což je cenné zejména při řešení bezpečnostních incidentů nebo provozních problémů.

V budoucnu by mohlo být přínosné rozšířit možnosti správy uživatelských účtů například o detailnější auditovací mechanismy, integraci s Lightweight Directory Access Protocol (LDAP) nebo Active Directory, a také o možnost vytvářet vlastní uživatelské role s přesně definovanými právy. Tato funkcionalita by dále zvýšila flexibilitu systému a umožnila jeho lepší přizpůsobení konkrétním potřebám akademického prostředí.

Možnost přizpůsobení systému Flowmon různým rolím uživatelů se v testovaném prostředí ukázala jako zásadní pro efektivní a bezpečné používání monitorovacího řešení. Díky tomu bylo možné rozdělit odpovědnosti mezi správce, analytiku a bezpečnostní specialisty bez nutnosti poskytovat všem plný přístup k celému systému.

Přehlednost a sjednocení grafického rozhraní

Jedním z hlavních přínosů systému Flowmon je přehledné a konzistentní grafické uživatelské rozhraní (GUI), které umožňuje intuitivní práci s daty, jejich analýzu a následné vyhodnocování bezpečnostních incidentů i provozních anomálií. Grafické rozhraní systému Flowmon je navrženo tak, aby bylo přístupné jak pro technicky zdatné uživatele, jako jsou administrátoři nebo bezpečnostní analytici, tak pro méně zkušené uživatele, kteří využívají systém především k základnímu monitoringu a generování reportů.

Rozhraní Flowmon je sjednoceno do webového přístupu přes zabezpečený protokol HTTPS, což umožňuje přístup z různých zařízení bez nutnosti instalace klientského softwaru. Tento přístup nejen zjednodušuje používání systému, ale také výrazně přispívá k jeho univerzální dostupnosti v rámci celé akademické sítě.

Struktura rozhraní

Grafické rozhraní Flowmon je členěno do několika hlavních modulů, které jsou přehledně uspořádány a dostupné prostřednictvím hlavního menu. Klíčovými moduly jsou:

Monitoring Center: Slouží k zobrazování statistik o síťovém provozu v reálném čase, generování přehledů o tokových datech, analýze historických dat a tvorbě reportů. Uživatelé mají přístup k interaktivním grafům a tabulkám, které umožňují rychlé filtrování a přizpůsobení zobrazených dat dle aktuálních potřeb.

ADS: Tento modul poskytuje přehled o všech detekovaných anomáliích a bezpečnostních incidentech. Rozhraní ADS nabízí možnosti přímého zásahu do detekčních pravidel, jejich úprav a možnosti vyhodnocení jednotlivých incidentů.

Reporting a Exporty: V tomto modulu je možné vytvářet automatizované reporty, exportovat data ve formátech jako CSV, JSON nebo PDF a odesílat je e-mailem na definované adresy.

Nastavení a správa uživatelů: Tento modul slouží administrátorům pro konfiguraci systému, správu uživatelských účtů, přístupových práv a nastavení importovaných blacklistů nebo definic detekčních pravidel.

Přehlednost a konzistence

Jednotlivé moduly systému Flowmon sdílejí konzistentní designové prvky, což výrazně přispívá k uživatelské přívětivosti. Klíčové vlastnosti, které zajišťují přehlednost rozhraní, zahrnují:

- **Jednotná barevná paleta a styl grafů:** Díky tomu jsou různé části systému vizuálně propojeny a uživatelé se v nich snadno orientují.
- **Interaktivní grafy a tabulky:** Grafy jsou klikatelné a umožňují přechod na detailní pohledy na konkrétní provoz, což usnadňuje analýzu a diagnostiku.
- **Možnost přizpůsobení dashboardů:** Uživatelé si mohou přizpůsobit hlavní obrazovky dle svých potřeb, což je důležité zejména pro bezpečnostní specialisty a správce sítě.
- **Responsivní design:** Webové rozhraní je optimalizováno pro různé velikosti obrazovek, což umožňuje přístup i z mobilních zařízení nebo vzdálených počítačů.

Přestože je rozhraní Flowmon hodnoceno jako přehledné a intuitivní, existuje několik oblastí, které by mohly být dále vylepšeny:

- **Možnost uživatelských profilů:** Umožnění každému uživateli přizpůsobit si rozhraní dle vlastních preferencí by přispělo k efektivnější práci s nástrojem, zejména pokud se systém používá na pravidelné bázi.
- **Rozšíření možností vizualizace:** Přidání nových typů grafů, jako jsou teplotní mapy nebo korelační diagramy, by mohlo výrazně zlepšit schopnost detekovat neobvyklé chování nebo anomálie.
- **Automatická doporučení:** Integrace nástrojů pro strojové učení, které by automaticky navrhovaly změny detekčních pravidel nebo vytvářely varování na základě historických trendů.

Podpora intuitivní navigace a zkratk

Jedním z klíčových prvků efektivního systému pro monitorování a správu sítí je intuitivní navigace, která umožňuje uživatelům rychle přistupovat k požadovaným funkcím a přehledům. Flowmon Monitoring Center poskytuje uživatelům komplexní prostředí, které bylo navrženo tak, aby jeho používání bylo co nejjednodušší a co nejefektivnější. Přestože se jedná o robustní nástroj se širokými možnostmi analýzy a detekce, jeho grafické rozhraní podporuje jednoduché ovládání pomocí intuitivních prvků a zkratk.

Rozhraní Flowmon Monitoring Center je rozčleněno do několika klíčových modulů, které jsou přístupné prostřednictvím hlavního menu. Mezi nejdůležitější části patří například dashboardy a přehledy, které umožňují rychlý přístup k hlavním statistikám síťového provozu, jako jsou Top Hosts, Top Protocols nebo Top Conversations. Tyto přehledy poskytují okamžitý přehled o nejvýznamnějších komunikačních tocích v síti.

Modul Monitoring Center slouží jako centrální bod pro analýzu tokových dat a zobrazení podrobných přehledů, které lze filtrovat podle časového období, typu protokolu, IP adres nebo konkrétní VLAN. Samostatnou součástí rozhraní je také ADS, jenž slouží k detekci anomálií a bezpečnostních incidentů a je dostupný přímo z hlavního menu.

Dále je k dispozici sekce pro nastavení a správu uživatelů, která umožňuje úpravu detekčních pravidel, práci s blacklisty nebo definování uživatelských rolí podle oprávnění. Celé rozhraní je navrženo s důrazem na přehlednost a snadnou orientaci, přičemž na všech obrazovkách jsou dostupná kontextová menu a nástroje pro rychlé filtrování a přizpůsobení zobrazovaných informací.

Podpora zkratk a urychlení navigace

Flowmon Monitoring Center nabízí i několik způsobů, jak zrychlit práci s rozhraním pomocí různých navigačních zkratk:

Klikací grafy a tabulky: Umožňují rychlý přechod na detailní přehledy o konkrétních prvcích sítě, například IP adresách nebo protokolech. Kliknutím na IP adresu v tabulce „Top Hosts“ se uživatel dostane přímo na detaily o komunikaci tohoto zařízení.

Uživatelsky definované filtry: Možnost uložit předem definované filtry pro opakované použití. Tento nástroj výrazně zjednodušuje analýzu typických provozních scénářů nebo hledání specifických typů provozu.

Klávesové zkratky: Přestože Flowmon Monitoring Center neobsahuje přímo klávesové zkratky, je možné v rámci prohlížeče používat standardní zkratky (např. Ctrl+F pro vyhledávání), což usnadňuje práci s dlouhými seznamy nebo složitými přehledy.

Přímý export dat: Možnost rychlého exportu přehledů do formátů CSV, JSON nebo PDF jediným kliknutím. To usnadňuje přenos dat do dalších nástrojů nebo jejich archivaci.

Lokalizace, dokumentace a jazyková podpora

Při zavádění pokročilých nástrojů pro monitoring síťového provozu, jako je systém Flowmon, musí být zvláštní pozornost věnována dostupnosti lokalizace, kvalitní dokumentace a široké jazykové podpoře. Tato oblast je zvlášť významná v prostředí vysokých škol, kde se s systémem pracuje napříč různými uživatelskými skupinami – od síťových administrátorů po technicky méně zkušené uživatele.

Bylo zjištěno, že nedostatečná lokalizace může vést k nesprávné interpretaci funkcí a následně i k chybnému nastavení systémových komponent. V případě Flowmonu se jedná o nástroj, jehož uživatelské rozhraní je standardně dodáváno v anglickém jazyce, což může být pro část uživatelů limitující. Proto by mělo být zváženo zavedení plnohodnotné české lokalizace, která by umožnila jednodušší přístup především administrativním pracovníkům a méně technickým uživatelům.

Dále by měla být kladena důrazná pozornost na dostupnost dokumentace v českém jazyce. Přestože jsou dostupné rozsáhlé manuály v angličtině, ukázalo se jako přínosné zajistit překlad klíčových částí dokumentace do češtiny, a to zejména v oblastech popisujících konfiguraci detekčních pravidel, práci s vizualizacemi a vytváření reportů. Pro zvýšení

dostupnosti informací by mohly být vytvořeny také interaktivní návody nebo video tutoriály, které by uživatelům poskytly názorné ukázky práce s jednotlivými moduly systému.

V neposlední řadě by mohla být zřízena online komunita nebo diskusní fórum v českém jazyce, kde by si uživatelé mohli vyměňovat zkušenosti, sdílet osvědčené postupy a konzultovat specifické problémy. Tím by se podpořila kolektivní znalostní báze a zefektivnilo by se řešení každodenních provozních situací.

Z výše uvedeného vyplývá, že důraz na lokalizaci, kvalitní dokumentaci a jazykovou podporu je v případě systému Flowmon nezbytnou součástí jeho úspěšného nasazení a efektivního využívání v akademickém prostředí.

Navigace a rychlý přístup

Přestože současná struktura menu v prostředí systému Flowmon umožňuje relativně intuitivní přístup ke všem dostupným modulům, v praxi se ukázalo, že při práci v krizových situacích může být orientace zpomalována absencí rychlých odkazů či klávesových zkratk. Tato skutečnost se projevuje zejména při nutnosti rychlého přepínání mezi jednotlivými přehledy nebo při vyhledávání specifických síťových toků.

Z tohoto důvodu by měla být zvážena implementace personalizovaných dashboardů, jejichž struktura by mohla být nastavena individuálně každým uživatelem. V takto přizpůsobeném rozhraní by bylo možné definovat vlastní sadu klíčových metrik, vizualizací a přehledů, čímž by se zrychlil přístup k nejčastěji používaným nástrojům a současně by se snížilo kognitivní zatížení při analýze incidentů.

Dále by mělo být do systému integrováno rozšíření o klávesové zkratky, které by umožnily efektivní provádění opakujících se úkonů – jako je například export dat, přepínání mezi jednotlivými časovými obdobími nebo aktivace konkrétních filtrů. Zavedením těchto prvků by bylo možné významně zkrátit reakční dobu administrátorů v případě výskytu kritických událostí a zároveň zvýšit komfort při každodenním používání systému.

Vizualizace dat a interaktivní grafy

Ačkoli jsou v systému Flowmon již nyní dostupné nástroje pro základní vizualizaci dat, jejich stávající možnosti by mohly být dále rozšířeny směrem k pokročilejší interaktivní analýze. Zejména by se měla zaměřit pozornost na zavedení grafických výstupů, které by uživateli umožnily intuitivní zoomování, filtrování jednotlivých datových vrstev

a interaktivní označování podezřelých nebo zajímavých událostí přímo v rámci vizualizačního prostředí.

Tímto způsobem by mohlo být dosaženo nejen zvýšení přehlednosti prezentovaných dat, ale i zefektivnění samotného procesu analýzy. Schopnost rychle identifikovat relevantní jevy a navázat na ně další analytické kroky je zvláště přínosná při zkoumání bezpečnostních incidentů, které se v síťovém provozu často projevují pouze jemnými odchylkami od běžného chování.

Další možností, jak tuto oblast dále rozvíjet, je implementace funkcí pro korelaci událostí napříč různými časovými obdobími. Takový nástroj by umožnil sledovat vývoj anomálií v čase, porovnávat konkrétní metriky mezi různými VLAN segmenty a tím lépe pochopit souvislosti mezi jednotlivými incidenty. Výsledkem by bylo nejen přesnější vyhodnocení bezpečnostních událostí, ale také vyšší úroveň prediktivní analytiky, která by mohla napomoci včasnému odhalení trendů naznačujících vznikající hrozby.

Celkově lze konstatovat, že rozšířením vizualizačních možností o dynamické, interaktivní a korelační prvky by bylo možné významně zvýšit uživatelskou přívětivost systému a podpořit efektivní rozhodování v oblasti síťové bezpečnosti.

Integrace s SIEM systémy

Jedním z hlavních směrů rozvoje systému Flowmon je integrace s platformami typu SIEM (Security Information and Event Management), mezi něž patří například Splunk, IBM QRadar nebo ArcSight. Tyto nástroje jsou využívány pro centralizovaný sběr, korelaci a analýzu bezpečnostních událostí z různorodých systémů a zařízení v síťové infrastruktuře.

Modul Flowmon ADS v tomto ohledu představuje důležitý zdroj informací, jelikož je schopen generovat detailní záznamy o síťovém provozu, detekovaných anomáliích a potenciálních bezpečnostních hrozbách. Propojením s SIEM systémy se nabízí možnost tyto výstupy automatizovaně předávat do centrálního monitorovacího prostředí. Tím se nejen zajišťuje komplexní pohled na dění v síti, ale zároveň se umožňuje korelace těchto údajů s logy z jiných zařízení – jako jsou servery, firewally nebo antivirová řešení.

Výsledkem této integrace je generování komplexních reportů, které pokrývají jak síťovou, tak aplikační vrstvu, a poskytují tak analytikům bezpečnosti důležité souvislosti. Kromě zajištění přehledného monitoringu v reálném čase může být díky integraci umožněna i automatizovaná reakce na incidenty – například ve formě okamžitého zablokování IP

adresy, vytvoření tiketu v systému správy událostí nebo rozeslání varovných e-mailových hlášení.

Aby mohla být integrace provedena efektivně, je doporučeno využívat standardizované formáty a komunikační protokoly, jako jsou Syslog, JSON API nebo REST API, které jsou systémem Flowmon nativně podporovány. Důraz by měl být rovněž kladen na nastavení autentizace a zabezpečeného přenosu dat, aby byla zajištěna důvěrnost a integrita předávaných informací. Celkově lze tuto formu integrace považovat za zásadní krok ke sjednocení bezpečnostní správy a zvýšení efektivity reakce na incidenty v prostředí univerzitní sítě.

Integrace s firewally a IDS/IPS systémy

Další klíčovou oblastí rozvoje systému Flowmon je jeho hlubší integrace s aktivními bezpečnostními prvky, zejména s firewally a systémy typu IDS/IPS. V rámci testovaného prostředí byly již využívány síťové prvky podporující protokol NetFlow v9, který umožňoval export síťových toků do systému Flowmon. Pro zajištění efektivní obrany proti síťovým hrozbám by však mělo být přistoupeno ke zřízení přímé komunikační vazby mezi modulem Flowmon ADS a konkrétními bezpečnostními zařízeními.

Jednou z možností je propojení Flowmonu s platformami jako Fortinet FortiGate, Palo Alto Networks nebo Cisco ASA. Tyto firewally umožňují import bezpečnostních pravidel, která mohou být generována na základě anomálií detekovaných systémem Flowmon. V praxi by tak mohla být detekovaná podezřelá komunikace automaticky blokována nebo jinak mitigována bez nutnosti manuálního zásahu administrátora.

Další možností je integrace se systémy typu Snort nebo Suricata, které slouží jako detekční a případně i preventivní mechanismy v síti (IDS/IPS). V tomto případě by výstupy z Flowmonu sloužily jako vstupní informace pro generování pravidel v těchto nástrojích. Na základě detekovaných anomálií by tak mohlo být přistoupeno k okamžitému blokování podezřelých spojení, případně ke generování varování směrem k administrátorům nebo SIEM systémům.

Implementací tohoto propojení by bylo dosaženo rychlé a automatické reakce na bezpečnostní incidenty, čímž by se výrazně zkrátila doba mezi detekcí a reakcí na hrozbu. Tímto způsobem by se posílil celkový bezpečnostní rámec univerzitní sítě a zároveň by se snížila zátěž na lidské zdroje v oblasti incident response. Integrace Flowmonu s firewally

a IDS/IPS nástroji tak představuje konkrétní a realizovatelný krok ke zvýšení úrovně ochrany síťové infrastruktury.

Integrace s DDoS ochrannými službami

Vzhledem k tomu, že součástí systému Flowmon je i modul Flowmon DDoS Defender, je vhodné, aby byla jeho funkcionalita rozšířena o přímé propojení s externími scrubbing centry a ochrannými službami typu Cloudflare, Akamai nebo Radware. Cílem takového propojení je zajistit, aby detekované DDoS útoky mohly být automatizovaně mitigovány v reálném čase bez nutnosti zásahu administrátora.

Aby mohlo být této integrace dosaženo, je nejprve třeba zajistit správné nastavení detekčních parametrů v modulu DDoS Defender. Systém musí být schopen přesně identifikovat objem útoku, zdrojové IP adresy a použité protokoly. Tyto údaje musí být následně exportovány ve strukturované podobě, která je kompatibilní s rozhraním příslušné externí ochranné platformy. Nejčastěji bývá využíván formát JSON či standardizovaný výstup pomocí protokolu Syslog, přičemž přenos těchto dat musí být zabezpečen, ideálně prostřednictvím šifrovaného API.

Po detekci a exportu incidentních údajů je možné přistoupit k automatickému přesměrování síťového provozu do scrubbing centra. Tento krok se provádí typicky prostřednictvím technik jako je Protokol hraniční brány (BGP) route injection nebo Generic Routing Encapsulation (GRE) tunneling. Je nezbytné, aby byla tato konfigurace předem projednána s poskytovatelem síťové konektivity univerzity, který musí podporovat přesměrování provozu na základě pravidel přijatých z Flowmonu.

Po úspěšném přesměrování provozu dochází k jeho očištění v rámci scrubbing centra. Získaný čistý provoz je následně navrácen zpět do univerzitní sítě, a to již bez škodlivých toků, které byly v externím systému odfiltrovány. Po ukončení útoku je doporučeno provést zpětnou kontrolu provozu a vyhodnotit účinnost celé mitigace. Záznamy z Flowmonu i z cloudového řešení by měly být porovnány a archivovány pro účely budoucí optimalizace detekčních pravidel.

V testovaném prostředí bylo potvrzeno, že propojením Flowmonu s externím scrubbing centrem lze dosáhnout výrazného zkrácení doby reakce na útok a minimalizace jeho dopadu. Tento přístup se tak jeví jako velmi vhodný zejména pro prostředí univerzitní sítě, kde je stabilita poskytovaných služeb zásadní a kde není žádoucí přetěžovat lidské kapacity správou incidentů, které mohou být řešeny automatizovaně.

Možnosti vylepšení integrace

Na základě zjištění z testovaného prostředí byly navrženy konkrétní kroky, které mohou vést k efektivnější integraci systému Flowmon s dalšími bezpečnostními nástroji. Cílem těchto opatření je vytvořit jednotný a konzistentní bezpečnostní ekosystém, který umožní přesnější korelaci událostí a centralizovanou správu incidentů v celé síťové infrastruktuře.

Integrace Flowmonu s dalšími systémy by měla být postavena na využití rozhraní REST API. V první fázi by měl být zajištěn přístup k oficiální dokumentaci tohoto rozhraní a následně by měla být ověřena jeho kompatibilita s cílovými systémy, jako jsou například SIEM platformy Splunk nebo IBM QRadar a bezpečnostní brány jako Palo Alto nebo Fortinet. Následně by měl být nakonfigurován export dat ve formátu kompatibilním se SIEM systémy (například JSON nebo CEF), včetně nastavení autentizačních mechanismů pro bezpečný přístup k API. V dalším kroku by měly být vytvořeny testovací scénáře pro ověření správného přenosu incidentů a jejich zobrazení v příslušných nástrojích.

Dalším doporučeným rozšířením je propojení systému Flowmon s nástroji pro správu zranitelností, například Nessus nebo OpenVAS. V rámci tohoto kroku by měly být pravidelně exportovány seznamy zranitelností z těchto nástrojů ve formátu XML nebo JSON a následně propojeny s daty detekovanými systémem Flowmon. Tato korelace umožní například automatické označování incidentů jako prioritních, pokud se komunikace uskuteční ze zařízení, u kterého byla zjištěna kritická zranitelnost.

Za účelem zvýšení přehlednosti a zefektivnění dohledu nad bezpečnostní situací v síti by měl být vybudován centralizovaný dashboard, který by zobrazoval data nejen z Flowmonu, ale také z ostatních nástrojů. Nejprve by měla být zvolena platforma pro vizualizaci (např. Grafana nebo Kibana) a následně vytvořen datový most propojující Flowmon, SIEM a případné další zdroje dat. Poté by měly být navrženy přehledy a metriky, které budou zobrazovat objem provozu, detekované hrozby, stav síťových prvků a výskyt zranitelností. V neposlední řadě by měly být definovány uživatelské pohledy podle potřeb jednotlivých rolí – od administrátorů až po vedení fakulty.

Posledním doporučením je zajištění pravidelné aktualizace blacklistů a detekčních pravidel na základě důvěryhodných externích zdrojů, jako jsou Spamhaus, AbuseIPDB nebo Talos. Tato aktualizace by měla být zajištěna prostřednictvím automatizovaných skriptů, které budou běžet v rámci plánovaných úloh (např. pomocí cron jobů nebo PowerShell skriptů). Při každé aktualizaci by měla být ověřena integrita stažených seznamů a veden záznam

o provedených změnách. Účinnost aktualizovaných pravidel by měla být následně vyhodnocována na měsíční bázi, a to zpětnou analýzou incidentů a porovnáním s historickými daty.

Díky těmto krokům může být dosaženo vyšší míry automatizace, lepší přehlednosti a celkové efektivity bezpečnostního dohledu v rámci univerzitní sítě. Integrace Flowmonu s ostatními nástroji tak představuje klíčový krok k vytvoření robustního bezpečnostního rámce.

7 ZÁVĚR PRAKTICKÉ ČÁSTI

Praktická část této práce se zaměřila na nasazení a testování systému Flowmon v prostředí univerzitní sítě Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Testování bylo provedeno na reálné infrastruktuře zahrnující směrovače, přepínače a bezdrátové přístupové body, přičemž cílem bylo ověřit schopnosti systému Flowmon v oblasti monitorování síťového provozu, detekce anomálií a reakce na bezpečnostní incidenty.

Pro nasazení systému Flowmon byly využity moduly Monitoring Center a ADS, které společně poskytly ucelený přehled o provozu v síti a umožnily detekovat různé typy anomálií a bezpečnostních incidentů. V rámci testování byly analyzovány síťové toky generované běžným provozem, přičemž byla sledována jak komunikace mezi jednotlivými VLAN, tak přístupy do internetu.

Monitoring Center se osvědčilo jako spolehlivý nástroj pro přehlednou vizualizaci a analýzu provozních statistik. Umožnilo identifikaci nejvytíženějších zařízení, dominantních protokolů a přenosů v různých částech sítě. Díky funkcím pro export dat a tvorbu automatizovaných reportů bylo možné poskytovat správcům sítě pravidelné přehledy o provozu a vytížení infrastruktury.

Modul Flowmon ADS prokázal svou užitečnost při detekci anomálií založených na behaviorální analýze. Byly zachyceny incidenty typu pokusů o neautorizovaný přístup, podezřelé DNS dotazy a nestandardní komunikace mezi zařízeními. Ačkoli nebyly všechny detekované události skutečně nebezpečné, systém poskytl užitečné nástroje pro jejich analýzu a vyhodnocení. Tento přístup umožnil nejen identifikovat bezpečnostní hrozby, ale také optimalizovat provozní nastavení sítě.

Praktická část rovněž prokázala schopnost systému Flowmon se efektivně integrovat do stávající infrastruktury univerzity, aniž by bylo nutné provádět složité změny nebo zásahy do konfigurace síťových zařízení. Virtuální appliance Flowmon Collector a Flowmon Probe byly snadno nasazeny v prostředí VMware, přičemž toková data byla exportována pomocí protokolů NetFlow v9 a IPFIX.

Přestože byl systém Flowmon v akademickém prostředí velmi užitečný, testování odhalilo i několik omezení. Zejména se jednalo o absenci podpory některých moderních aplikačních protokolů na úrovni L7 a omezené možnosti vizualizace v rámci stávajících dashboardů.

Rovněž byla zaznamenána určitá míra falešně pozitivních detekcí v modulu ADS, což může vést k nutnosti dodatečné konfigurace a optimalizace detekčních pravidel.

Celkově však systém Flowmon v testovaném prostředí splnil očekávání a poskytl důležité informace pro optimalizaci provozu a zajištění bezpečnosti univerzitní sítě. V další fázi vývoje by bylo vhodné zaměřit se na zlepšení uživatelského rozhraní, rozšíření podpory aplikačních protokolů a vylepšení mechanismů automatické reakce na detekované incidenty. Flowmon tak představuje robustní a adaptabilní nástroj, který může být cenným přínosem pro správu a ochranu sítí nejen v akademickém prostředí, ale i v dalších organizacích s rozsáhlou infrastrukturou.

ZÁVĚR

Tato diplomová práce se zaměřila na analýzu, implementaci a vyhodnocení monitorovacího systému Flowmon v akademickém prostředí Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Cílem práce bylo ověřit účinnost platformy Flowmon při detekci síťových hrozeb, anomálií a optimalizaci výkonu sítě v rámci univerzitní infrastruktury.

V teoretické části byly popsány základy síťového monitorování, metody detekce hrozeb a současné trendy v oblasti kybernetické bezpečnosti. Dále byla představena architektura systému Flowmon, jeho klíčové komponenty a jejich principy fungování. Součástí teoretické části bylo také srovnání s dalšími monitorovacími řešeními, které jsou běžně používány v podnikových a akademických sítích.

Praktická část práce se věnovala implementaci systému Flowmon do univerzitní sítě a následné analýze nasbíraných dat. Bylo provedeno nasazení hlavních modulů Flowmonu – Monitoring Center a ADS, které byly konfigurovány k nepřetržitému monitorování provozu a detekci bezpečnostních incidentů. V rámci testování byly sledovány především problémy spojené s přetížením infrastruktury, nesprávným nastavením síťových segmentů a výskytem potenciálně škodlivého provozu.

Výsledky testování potvrdily, že systém Flowmon je schopen efektivně detekovat různé typy anomálií, včetně neautorizovaného přístupu, síťového skenování nebo neobvyklého provozu v jednotlivých VLAN. Modul ADS se ukázal jako užitečný nástroj pro identifikaci bezpečnostních incidentů na základě heuristických metod a strojového učení. Dále bylo zjištěno, že implementace systému Flowmon přináší významné přínosy v oblasti monitorování výkonu sítě, zejména díky schopnosti analyzovat dlouhodobé trendy a optimalizovat provoz na základě zjištěných statistik.

Mezi hlavní výhody systému Flowmon patří jeho flexibilita, modularita a schopnost detekovat i neznámé hrozby pomocí behaviorální analýzy. Významným přínosem je také jeho schopnost integrace s dalšími bezpečnostními nástroji a široká škálovatelnost umožňující nasazení v různě velkých sítích. Na druhou stranu byly identifikovány i určité nedostatky, zejména v oblasti uživatelské přívětivosti a komplexnosti konfigurace jednotlivých modulů.

Na základě provedených testů a analýz byly navrženy konkrétní kroky ke zlepšení efektivity systému, včetně automatizace reakce na incidenty, rozšíření podpory aplikačních protokolů na vrstvě L7 a vylepšení uživatelského rozhraní.

Flowmon se ukázal jako vhodné řešení pro monitorování akademické sítě a jeho implementace přinesla významné zlepšení nejen v oblasti bezpečnosti, ale i provozního dohledu. V budoucnu bude vhodné se zaměřit na další rozvoj systému, zejména na automatizaci detekce a reakce na hrozby, integraci s dalšími nástroji pro kybernetickou bezpečnost a zjednodušení jeho správy pro různé typy uživatelů.

SEZNAM POUŽITÉ LITERATURY

ARBOR NETWORKS. *DDoS Protection and Network Visibility Solutions*. Arbor Networks, 2023. Dostupné z: <https://www.netscout.com/arbor>.

BEJTILICH, Richard. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. San Francisco: No Starch Press, 2020. ISBN 978-1-59327-509-9.

CISCO. *NetFlow and IPFIX for Deep Network Visibility*. Cisco Systems, 2023. Dostupné z: <https://www.cisco.com>.

CISCO. *NetFlow and IPFIX Monitoring for Enterprise Security*. Cisco Systems, 2023. Dostupné z: <https://www.cisco.com>.

CISCO STEALTHWATCH. *Network Visibility and Security Analytics*. Cisco, 2023. Dostupné z: <https://www.cisco.com>.

COLLINS, Michael. *Network Security Through Data Analysis: From Data to Action*. 2nd ed. Beijing: O'Reilly Media, 2017. ISBN 978-1-491-96284-8.

DARKTRACE. *AI-Driven Threat Detection for Enterprise Security*. Darktrace, 2023. Dostupné z: <https://www.darktrace.com>.

ENISA. *NIS2 Directive: Strengthening EU Cybersecurity Regulations*. European Union Agency for Cybersecurity, 2023. Dostupné z: <https://www.enisa.europa.eu>.

ENISA. *Threat Landscape Report 2023: Key Trends and Emerging Threats*. European Union Agency for Cybersecurity, 2023. Dostupné z: <https://www.enisa.europa.eu>.

EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2023*. Europol, 2023. Dostupné z: <https://www.europol.europa.eu>.

FIREYE. *Advanced Persistent Threats: 2023 Report on Evolving Cyber Threats*. FireEye, 2023. Dostupné z: <https://www.fireeye.com>.

FLOWMON. *Detekce neznámých hrozeb*. Online. Brno: Flowmon, 2025 [cit. 2025-03-03]. Dostupné z: <https://flowmon.com/cs/solutions/security-operations/unknown-threat-detection>.

FLOWMON. *Monitorování NetFlow / IPFIX*. Online. Brno: Flowmon, 2025 [cit. 2025-03-03]. Dostupné z: <https://www.flowmon.com/cs/solutions/network-and-cloud-operations/netflow-ipfix>.

FLOWMON NETWORKS. *DDoS Defender: Real-Time Protection Against Distributed Denial of Service Attacks*. Progress, 2021. Dostupné z: <https://www.flowmon.com>.

FLOWMON NETWORKS. *Flowmon and AI-Powered Threat Detection: Enhancing Cybersecurity with Behavioral Analytics*. Progress, 2023. Dostupné z: <https://www.flowmon.com>.

FLOWMON NETWORKS. *Flowmon Anomaly Detection System: Technical Whitepaper*. Progress, 2023. Dostupné z: <https://www.flowmon.com>.

FLOWMON NETWORKS. *Flowmon in Zero Trust Security Architectures*. Progress, 2023. Dostupné z: <https://www.flowmon.com>.

GARTNER. *Top Trends in Cybersecurity 2023*. Gartner Research, 2023. Dostupné z: <https://www.gartner.com>.

KOLOUCH, Jan. *CyberSecurity*. Edice CZ.NIC. 2019. ISBN 978-80-88168-31-7.

MORGAN, Steve. *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*. Cybersecurity Ventures, 2022. Dostupné z: <https://cybersecurityventures.com>.

PROGRESS. *Cloud Security and Network Monitoring with Flowmon*. Progress, 2023. Dostupné z: <https://www.progress.com>.

PROGRESS. *Flowmon Integration with SIEM and Security Ecosystems*. Progress, 2021. Dostupné z: <https://www.progress.com>.

SCHNEIER, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley, 2021. ISBN 978-0-47-145380-2.

STALLINGS, William. *Network Security Essentials: Applications and Standards*. 6th edition. Boston: Pearson, 2020. ISBN 978-0-13-452733-8.

ZHANG, Tianzhu; LINGUAGLOSSA, Leonardo; GALLO, Massimo; GIACCONE, Paolo a ROSSI, Dario. *FlowMon DPDK: Parsimonious Per-Flow Software Monitoring at Line Rate*. In: *2018 Network Traffic Measurement and Analysis Conference (TMA)*. 2018. ISBN 978-1-5386-7152-8.

SEZNAM OBRÁZKŮ

Obrázek 1: Detekce podezřelé komunikace přes šifrované spojení (TCP/443)	66
Obrázek 2: Konfigurace atomických filtrů	70
Obrázek 3: Souhrn detekovaných událostí a anomálií.....	71
Obrázek 4: Seznam detekovaných anomálií v období 17.–24. března 2025 – trend výskytu	72
Obrázek 5: „Blacklisty“	73
Obrázek 6: Časová osa detekovaných bezpečnostní metod v období 18.–24. března 2025	73
Obrázek 7: Přehled zařízení podle skóre ohrožení a detekovaných událostí.....	74
Obrázek 8: Přehled konkrétních bezpečnostních událostí	75
Obrázek 9: Seznam externích dotazů.....	78
Obrázek 10: Uživatelské rozhladní „False Positive“	79
Obrázek 11: Uživatelské rozhraní.....	98

SEZNAM TABULEK

Tabulka 1: TOP Hosts.....	52
Tabulka 2: Top Protocols.....	53
Tabulka 3: Top Conversations	53
Tabulka 4: Top VLANs	54
Tabulka 5: Funkce Flowmon Monitoring Center	57
Tabulka 6: Přehled protokolů a identifikovaných anomálií.....	64
Tabulka 7: Přehled detekovaných anomálií	65
Tabulka 8: FMEA analýza modulu Flowmon ADS.....	77
Tabulka 9: Přehled zjištěných omezení	84

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Zkratka	Anglický význam	Český význam
ACK	Acknowledgement	Potvrzení přijetí (paketu)
ACL	Access Control List	Seznam řízení přístupu
ADS	Anomaly Detection System	Systém pro detekci anomálií
AI	Artificial Intelligence	Umělá inteligence
API	Application Programming Interface	Programovací rozhraní aplikace
APT	Advanced Persistent Threat	Pokročilá perzistentní hrozba
ARP	Address Resolution Protocol	Protokol pro zjištění MAC adresy
BGP	Border Gateway Protocol	Protokol hraniční brány
C&C	Command and Control	Řídicí a kontrolní (server)
DDoS	Distributed Denial of Service	Distribuované odepření služby
DPDK	Data Plane Development Kit	Vývojová sada pro zpracování dat
DPI	Deep Packet Inspection	Hluboká analýza paketů
FMC	Firepower Management Center	Centrum pro správu Firepower (Cisco)
FMEA	Failure Mode and Effects Analysis	Analýza způsobů poruch a jejich důsledků
GRE	Generic Routing Encapsulation	Obecné zapouzdření směrování
GUI	Graphical User Interface	Grafické uživatelské rozhraní
HTTPS	HyperText Transfer Protocol Secure	Bezpečný přenos hypertextu
IoT	Internet of Things	Internet věcí
IPFIX	IP Flow Information Export	Export informací o IP tocích
IPS	Intrusion Prevention System	Systém prevence průniku
JA3	TLS Fingerprint Technique	Technika otisku TLS (pro detekci klientů)

Zkratka	Anglický význam	Český význam
JSON	JavaScript Object Notation	Formát pro strukturovaná data
LDAP	Lightweight Directory Access Protocol	Lehký adresářový přístupový protokol
MTU	Maximum Transmission Unit	Maximální přenosová jednotka
QoS	Quality of Service	Kvalita služby
RBAC	Role-Based Access Control	Řízení přístupu na základě rolí
RDP	Remote Desktop Protocol	Protokol pro vzdálenou plochu
sFlow	Sampled Flow	Vzorkovaný tok dat
SIEM	Security Information and Event Management	Správa bezpečnostních informací a událostí
SSH	Secure Shell	Bezpečné vzdálené připojení
TCP	Transmission Control Protocol	Řídicí přenosový protokol
UDP	User Datagram Protocol	Uživatelský datagramový protokol