**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**



# Diplomová práce

## Integrace DLP řešení s dalším bezpečnostním softwarem v podniku

**Veronika Jiráčková**

**© 2026 ČZU v Praze**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Veronika Jiráčková, DiS.

Informatika

Název práce

**Integrace DLP řešení s dalším bezpečnostním softwarem v podniku**

Název anglicky

**Integrating of DLP solution with other security software in the company.**

---

**Cíle práce**

Hlavním cílem této diplomové práce bude analyzovat a vyhodnotit integraci systému pro prevenci úniku dat (DLP) s podnikovým systémem pro správu bezpečnostních událostí (SIEM) se zaměřením na kvalitu přenášených dat a spolehlivost přenosu. Na základě výsledků analýzy a informací zjištěných z testovacích scénářů budou dle možností navrhnuta doporučení pro zvýšení efektivity procesů v oblasti incident response.

**Metodika**

V první části diplomové práce bude provedena literární rešerše související odborné literatury a charakteristika stávajícího stavu bezpečnostních systémů ve zvoleném podniku. Primární data, nad kterýma bude v druhé části práce provedena analýza, budou získána z logů DLP a SIEM systémů. Využity budou především kvantitativní metody výzkumu, konkrétně deskriptivní statistická metoda. Podpůrná data budou pocházet z případových studií vybraných scénářů.

**Doporučený rozsah práce**

60-80s.

**Klíčová slova**

DLP, SIEM, Data Loss Prevention, informační bezpečnost, prevence úniku dat, integrace systému, bezpečnostní systém, řízení bezpečnosti

---

**Doporučené zdroje informací**


BOUHALI, Wiâme, Elmostafa BELMEKKI and Mostafa BELLAFKIH, 2024. Advanced Techniques for Security Incident Analysis. – [online]. 1–6. Available at: doi:10.1109/wincom62286.2024.10654882

CINQUE, Marcello, Domenico COTRONEO and Antonio PECCHIA, 2018. Challenges and directions in Security Information and Event Management (SIEM). 2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) [online]. 95–99. Available at: doi:10.1109/issrew.2018.00-24

GONZÁLEZ-GRANADILLO, Gustavo, Susana GONZÁLEZ-ZARZOSA and Rodrigo DIAZ, 2021. Security Information and Event Management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors [online]. 21(14), 4759. Available at: doi:10.3390/s21144759

CHO, Hyunwoo and Keuntae CHO, 2025. Impact of security management activities on corporate performance. Systems [online]. 13(8), 633. Available at: doi:10.3390/systems13080633

PARACHA, Muhammad Arsalan, Muhammad SHEERAZ, Yuanyuan CHAI, Saad AHMAD, Zubair Nasir KHAN, Shah HUSSAIN, None AFTAB-UL-HAQ and Muhammad Hanif DURAD, 2022. Implementation of Two Layered DLP Strategies. – [online]. 8–13. Available at: doi:10.1109/iccws56285.2022.9998436

ROMANSKY, Radi P and Irina S NONINSKA, 2020. Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences & Engineering [online]. 17(5), 5288–5303. Available at: doi:10.3934/mbe.2020286


---

**Předběžný termín obhajoby**

2025/26 LS – PEF

**Vedoucí práce**

Ing. Martin Havránek, Ph.D.

**Garantující pracoviště**

Katedra informačních technologií

Elektronicky schváleno dne 18. 09. 2025

**doc. Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 30. 01. 2026

**prof. Ing. Lukáš Čechura, Ph.D.**

Děkan

V Praze dne 07. 03. 2026

**Čestné prohlášení**

Prohlašuji, že svou diplomovou práci " Integrace DLP řešení s dalším bezpečnostním softwarem v podniku" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. 3. 2026 _____

**Poděkování**

Ráda bych touto cestou poděkovala Ing. Martinu Havránkovi, Ph.D., za odborný dohled a vedení mé diplomové práce. Zároveň bych také chtěla poděkovat zkoumanému podniku a jeho zaměstnancům za pomoc a ochotu při sběru dat.

# Integrace DLP řešení s dalším bezpečnostním softwarem v podniku


**Abstrakt**

Diplomová práce se zabývá problematikou integrace systému pro prevenci úniku dat (DLP) s podnikovým systémem pro správu bezpečnostních informací a událostí (SIEM). Hlavním cílem práce je analyzovat kvalitu a spolehlivost přenosu bezpečnostních událostí mezi těmito systémy a na základě získaných poznatků navrhnout doporučení pro zlepšení procesů v oblasti řízení bezpečnostních incidentů.

Teoretická část práce se zaměřuje na oblast podnikové informační bezpečnosti, identifikaci kybernetických hrozeb, přehled relevantních standardů a legislativních požadavků a popis architektury bezpečnostních systémů. Dále jsou detailně charakterizovány systémy DLP a SIEM, jejich principy fungování a metody detekce. Pozornost je věnována také problematice integrace bezpečnostních nástrojů a přenosu dat mezi nimi.

Praktická část práce analyzuje konkrétní implementaci DLP a SIEM v podnikovém prostředí a zaměřuje se na testování jejich vzájemné integrace. V rámci práce byly navrženy a realizovány testovací scénáře ověřující správnost parsování a mapování dat, úplnost přenosu událostí a chování systému při výpadku datového toku. Výsledky testování byly následně vyhodnoceny s ohledem na kvalitu dat a spolehlivost integrace.

Na základě provedené analýzy jsou formulována doporučení pro optimalizaci integrace DLP a SIEM systémů, zejména v oblasti zajištění kvality dat a řízení bezpečnostních incidentů.



**Klíčová slova:** DLP, SIEM, Data Loss Prevention, informační bezpečnost, prevence úniku dat, integrace systému, bezpečnostní systém, řízení bezpečnosti

# Integrating of DLP solution with other security software in the company

**Abstract**

This thesis examines the integration of a data loss prevention (DLP) system with an enterprise security information and event management (SIEM) system. The main objective of this thesis is to analyze the quality and reliability of security event transmission between these systems and, based on the findings, to propose recommendations for improving security incident management processes.

The theoretical part of this thesis focuses on corporate information security, the identification of cyber threats, an overview of relevant standards and legal requirements, and a description of security system architectures. It also provides a detailed analysis of DLP and SIEM systems, their operating principles, and detection methods. Furthermore, attention is given to the integration of security tools and data transfer between them.

The practical part of this thesis analyzes the specific implementation of DLP and SIEM in an enterprise environment and focuses on testing their integration. As part of this work, test scenarios were designed and implemented to verify the accuracy of data parsing and mapping, the completeness of event transmission, and the system's behavior in the event of a data stream failure. The test results were subsequently evaluated regarding data quality and the reliability of the integration.

Based on the analysis, recommendations are formulated for optimizing the integration of DLP and SIEM systems, particularly in the areas of data quality assurance and security incident management.

**Keywords**: DLP, SIEM, Data Loss Prevention, information security, data leak prevention, system integration, security system, security management

# Obsah

**1 Úvod ..... 11**

**2 Cíl práce a metodika ..... 12**

2.1 Cíl práce ..... 12

2.2 Metodika ..... 12

**3 Teoretická východiska ..... 13**

3.1 Podniková informační bezpečnost ..... 13

3.1.1 Kybernetické hrozby ..... 13

3.1.2 Normy a standardy ..... 18

3.1.3 Legislativní požadavky v EU a ČR ..... 19

3.1.4 Dopady kybernetických útoků ..... 21

3.1.5 Architektura bezpečnostních systémů podniku a standardní nástroje 22

3.2 DLP systémy ..... 26

3.2.1 Klasifikace dat ..... 26

3.2.2 Klasifikace DLP systémů ..... 27

3.2.3 Procesy a metody ..... 28

3.2.4 Přehled dostupných řešení ..... 29

3.3 SIEM ..... 29

3.3.1 Architektura SIEM ..... 30

3.3.2 Modely nasazení SIEM ..... 33

3.3.3 Metody detekce v SIEM ..... 34

3.3.4 SOC ..... 35

3.3.5 Přehled dostupných platforem ..... 37

3.4 Integrace bezpečnostních systémů ..... 38

3.4.1 Přenos dat mezi systémy ..... 38

3.4.2 Problémy spojené s integrací bezpečnostních systémů ..... 40

3.4.3 Příklady výzkumů integrace bezpečnostních systémů ..... 41

3.5 Vývoj a trendy v oblasti SIEM a DLP ..... 43

**4 Vlastní práce ..... 46**

4.1 Představení podniku ..... 46

4.2 Zkoumané podnikové systémy ..... 47

4.2.1 Podnikové operační centrum SOC ..... 47

4.2.2 Stávající DLP řešení ..... 47

4.2.3 Případová studie: bezpečnostní politika k ochraně obchodního tajemství 49

4.2.4 Stávající SIEM platforma ..... 52

4.2.5 Přenos dat v rámci podniku ..... 54

4.3 Cíle testování ... 57
4.3.1 Omezení při testování ... 57
4.4 TC-01 Validace parsování a kvality dat ... 58
4.4.1 Příprava testovacích politik ... 58
4.4.2 Průběh testu ... 63
4.5 TC-02 Chaos test: výpadek toku z DLP do SIEM ... 65
4.5.1 Příprava testovacích dat a systémů ... 65
4.5.2 Průběh testu ... 67

**5 Výsledky ... 69**
5.1 Výsledky TC-01 ... 69
5.1.1 Shrnutí výsledků TC-01 ... 71
5.2 Výsledky TC-02 ... 71
5.2.1 Shrnutí výsledků TC-02 ... 74
5.3 Doporučení podniku ... 75
5.3.1 Doporučení v návaznosti na TC-01 ... 75
5.3.2 Doporučení v návaznosti na TC-02 ... 75

**6 Závěr ... 78**

**7 Seznam použitých zdrojů ... 80**

**Seznam obrázků, tabulek, grafů a zkratek ... 85**
7.1 Seznam obrázků ... 85
7.2 Seznam tabulek ... 85
7.3 Seznam grafů ... 86

# 1 Úvod

V současné době jsou informační technologie nedílnou součástí fungování většiny organizací a podniků. Spolu s rostoucím objemem zpracovávaných dat a digitalizací podnikových procesů však narůstá i riziko kybernetických incidentů, zejména těch spojených s únikem citlivých informací. Organizace proto implementují komplexní bezpečnostní architektury tvořené různými specializovanými nástroji, které společně zajišťují detekci, prevenci a reakci na bezpečnostní události. Mezi významné technologie patří zejména systémy pro prevenci úniku dat Data Loss Prevention (DLP) a systémy pro správu bezpečnostních informací a událostí (SIEM), jejichž efektivní spolupráce může výrazně přispět k včasné identifikaci bezpečnostních incidentů a ochraně podnikových informací.

Teoretická část práce se zaměřuje na základní koncepty podnikové informační bezpečnosti a na přehled hlavních nástrojů používaných k ochraně dat v moderních organizacích. Nejprve jsou představeny současné kybernetické hrozby, standardy a legislativní požadavky související s ochranou informací. Následně je pozornost věnována architektuře podnikových bezpečnostních systémů a jednotlivým bezpečnostním technologiím. Detailněji jsou popsány systémy DLP, jejich principy fungování, metody detekce a klasifikace dat, a dále systémy SIEM, které umožňují centralizovaný sběr, korelaci a analýzu bezpečnostních událostí. Závěrečná část teoretických východisek se zabývá problematikou integrace bezpečnostních systémů, přenosem dat mezi nimi a současnými trendy v oblasti kybernetické bezpečnosti.

Na teoretická východiska navazuje praktická část práce, která se zaměřuje na analýzu integrace DLP řešení s podnikovou SIEM platformou v reálném prostředí organizace. Praktická část zahrnuje představení zkoumaného podniku a jeho bezpečnostní infrastruktury, zejména využívaného DLP systému a SIEM platformy. Následně jsou definovány testovací scénáře, jejichž cílem je ověřit kvalitu a spolehlivost přenosu bezpečnostních událostí mezi oběma systémy. Testování se soustředí zejména na správnost parsování a mapování dat, úplnost přenesených událostí a chování systému při dočasném přerušení datového toku a následném zpracování backlogu událostí. Výsledky těchto testů slouží jako podklad pro vyhodnocení funkčnosti integrace a pro formulaci doporučení pro zlepšení procesů v oblasti řízení bezpečnostních incidentů.

# 2 Cíl práce a metodika

## 2.1 Cíl práce

Hlavním cílem této diplomové práce bude analyzovat a vyhodnotit integraci systému pro prevenci úniku dat (DLP) s podnikovým systémem pro správu bezpečnostních událostí (SIEM) se zaměřením na kvalitu přenášených dat a spolehlivost přenosu. Na základě výsledků analýzy a informací zjištěných z testovacích scénářů budou dle možností navrhnuta doporučení pro zvýšení efektivity procesů v oblasti incident response.

## 2.2 Metodika

V první části diplomové práce bude provedena literární rešerše související odborné literatury a charakteristika stávajícího stavu bezpečnostních systémů ve zvoleném podniku. Primární data, nad kterýma bude v druhé části práce provedena analýza, budou získána z logů DLP a SIEM systémů. Využity budou především kvantitativní metody výzkumu, konkrétně deskriptivní statistická metoda. Podpůrná data budou pocházet z případových studií vybraných scénářů.

# 3 Teoretická východiska

## 3.1 Podniková informační bezpečnost

V dnešní době digitalizace je úspěšnost podniků zásadně závislá na informačních technologií, které daná firma používá. Je velký tlak na to, aby se veškerá data, od zákaznických databází až po interní know-how, přesunula do moderních IT systémů, nejlépe těch, co se nachází v cloudu. Každý den nezastavitelně narůstá už teď masivní objem světových dat, podle odborných odhadů z roku 2024 šlo o přibližně 402,74 milionu TB denně. (Bartley 2025)

Větší množství dat a více využívaných technologií ale vede i k větším bezpečnostním rizikům. V roce 2025 byla více jak polovina firem, které se účastnily výzkumu Cyber Readiness Report 2025, cílem kybernetického útoku. Následkem těchto útoků byly i pokuty, které musela zaplatit více jak jedna třetina z nich. (Hiscox 2025) Zároveň, když už k úniku dat dojde, jsou mnohem rozsáhlejší i samotné následky. Do dat sesbíraných mezi lety 2005 až 2018 bylo zahrnuto 8943 nahlášených úniků, které vedly ke ztrátě více než 10 miliard záznamů o zákaznících. (Markos et al. 2023)

Narůstající kybernetická rizika nejsou ale podnikům lhostejná. Z oslovených 5750 společností jich v posledních 12 měsících 94 % zvýšilo investici do kybernetické bezpečnosti a ochrany dat a 60 % najalo další zaměstnance pro tuto oblast. (Hiscox 2025) Výběr nástrojů a strategií pro zajištění dostatečné ochrany je ale ztěžovaný neustále se vyvíjející technologií, která se mění rychleji, než stačí bezpečnostní opatření reagovat. Na jednu stranu nové technologie umožňují podnikům zpracovávat obrovské množství dat, ale na druhou jsou to právě pokročilé technologie, které hackeři používají k sofistikovaným útokům

### 3.1.1 Kybernetické hrozby

Moderní přístupy k vykonávání práce, např. možnost pracovat na vlastních koncových zařízeních (BYOD), vedou k tomu, že je bezpečnostní perimetr firmy stále více proniknutelný. (De Sousa a Shahzad 2021) Do sítě je připojena směs různorodých koncových zařízení pracujících s citlivými údaji, které je potřeba chránit, ale zároveň nenarušovat pracovní procesy ve firmě.

Tradiční bezpečnostní opatření, jako jsou firewally nebo antivirové programy už v dnešní době nejsou dostačující bezpečnostní prvky pro moderní společnosti zpracovávající mohutné množství dat. Tyto programy neumožňují hloubkovou kontrolu obsahu a spoléhají se pouze na známé signatury, což není příliš účinné například proti aktivitě botnetů. (Huralnyk et al. 2025) Firmy potřebují budovat komplexní vícevrstvé bezpečnostní systémy, které jsou schopné se přizpůsobovat proměnlivým kybernetickým hrozbám.

Kybernetická rizika jsou dynamicky se vyvíjejícím problémem, který ohrožuje integritu, důvěrnost a dostupnost firemních systémů. Klasifikace těchto rizik pomáhá organizacím určit priority při zavádění bezpečnostních opatření. Kybernetické hrozby mohou pocházet z různých směrů a zdrojů, které mezi sebou často mívají úzké souvislosti a prolínají se. Jedním se způsobů, jak je rozdělit, je na:

- externí aktéry
- interní aktéry

## EXTERNÍ AKTÉŘI

Charles J. Brooks ve své knize Cybersecurity Essentials definuje několik typů lidí využívajících Internet a jedním z nich jsou i „špatní lidé, kteří chtějí získat přístup k počítačům za účelem krádeže informací, špionáže, nebo narušení komunikace“ (Brooks et al. 2018). Firmy zpravidla využívají své vlastní intranetové sítě, ty se ale setkávají s Internetem v bodech, které tvoří tzv. perimetr neboli hranici toho, kde má podnik ještě kontrolu a kde už ne. Nejčastějšími hrozbami, s kterými se podniky v dnešní době setkávají, jsou:

### Viry, červi a trojské koně

V kontextu kybernetických útoků na firmy představují útoky, které využívají hackování nebo malware jednu z nejčastějších metod narušení datové bezpečnosti. Podle analýzy dat z let 2005 až 2018 tvořilo hackování nebo malware v průměru 28 % všech incidentů. (Markos et al. 2023)

Viry jsou definovány jako destruktivní programy, jejichž primárním účelem je replikace a šíření v rámci lokálního koncového zařízení. Fungují na principu modifikace jiných počítačových programů, do kterých vkládají svůj vlastní kód, a tím dané oblasti „infikují“. K jejich replikaci dochází nejčastěji, když uživatelé stahují neověřené programy z Internetu nebo otevírají přílohy podezřelých e-mailů.

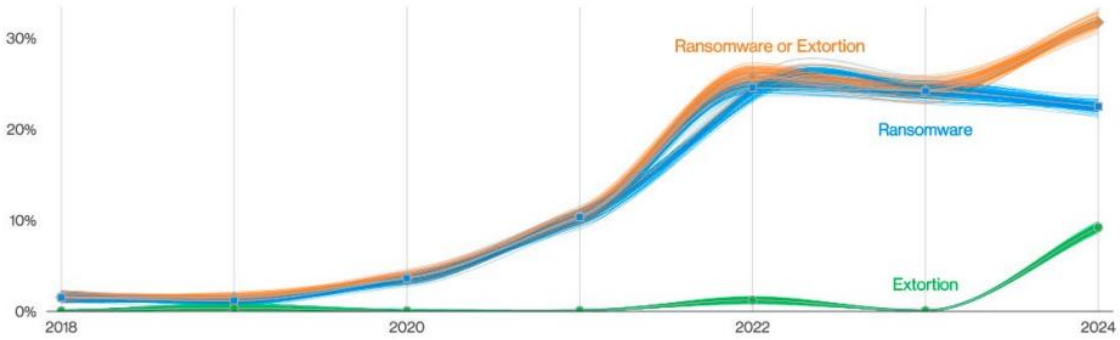
Červi, někdy označovaní jako síťové viry, se liší od klasických virů tím, že k infikování počítače nevyžadují hostitelský program. Šíří se především prostřednictvím síťového připojení a jejich mechanismus útoku spočívá ve vyhledávání zranitelností v aplikacích, které následně využívají k replikaci a šíření na další počítače v síti. (Ghillione 2024)

Trojské koně jsou typem malwaru, který maskuje svou pravou povahu tím, že se jeví jako legitimní a běžně používaná aplikace. Uživatelé jsou tak oklamáni k jejich spuštění v domnění, že jde o bezpečný software. Přestože program může navenek fungovat správně, obsahuje skrytý škodlivý kód, který se aktivuje při jeho spuštění

Ačkoliv jsou viry, červi a trojské koně samostatně definované jako destruktivní programy, jsou v moderních hrozbách často využívány jako součást komplexnějších útoků, které vedou k instalaci dalších forem malwaru, jako je ransomware. (Brooks et al. 2018).

**Ransomware**

Ransomware představuje jeden z nejzávažnějších a nejčastějších typů škodlivého softwaru, se kterým se dnes podnikové sítě setkávají. Podle reportu z roku 2024 přibližně jedna třetina všech narušení bezpečnosti v podnicích souvisela s ransomware nebo obdobnou technikou vydírání, jak je vidět v grafu 1. Ransomware byl nejčastější hrozbou v 92 % odvětví podniků, které se studie účastnily. (Verizon 2024)




*Graf 1 - Nárůst Ransomware útoků mezi lety 2018 až 2024*
*Zdroj: (Verizon 2024)*

Ransomware je software navržený tak, aby uzamkl systémy nebo zašifroval data uživatele, čímž znemožní přístup k zařízením, souborům nebo celým systémům. Útočník následně požaduje zaplacení výkupného (obvykle v kryptoměnách, jako je Bitcoin) za poskytnutí soukromého dešifrovacího klíče, který jako jediný dokáže data obnovit.

Nejběžnějším způsobem šíření ransomwaru je spamový e-mail (Brooks et al. 2018). Malware je aktivován, když uživatel klikne na infikovanou přílohu nebo odkaz obsažený ve zprávě. E-mailové útoky typu phishing využívají podvržené zprávy k oklamání uživatelů, aby prozradili citlivé informace nebo klikli na škodlivé odkazy, které ransomware stáhnou. Jinými způsoby šíření jsou například infikované webové stránky nebo kompromitovaný software.

Podle dalšího reportu z roku 2025 se ze společností, které čelily kybernetickému útoku, 29 % setkalo s ransomware. Přestože 60 % firem, které výkupné zaplatily, získalo zpět část nebo všechna svá data, platba nepřináší jistotu. U 31 % organizací, které výkupné uhradily, útočníci následně požadovali další finanční prostředky. Navíc 27 % těch, kteří zaplatili, utrpělo dodatečný útok, i když ne nutně od stejného útočníka. (Hiscox 2025)

**DoS/DDoS útoky**

Útoky Denial of Service (DoS) a Distributed Denial of Service (DDoS) jsou kritickými síťovými hrozbami, které primárně cílí na dostupnost dat, tedy na jeden ze tří pilířů informační bezpečnosti. Cílem těchto útoků je přetížení serveru nebo síťového zdroje do takové míry, že není schopen poskytovat své služby. Útoky DoS a

DDoS mohou být provedeny různými způsoby, přičemž jejich princip spočívá v zahlcení cíle masivním provozem nebo požadavky. Během druhého čtvrtletí roku 2025 společnost Cloudflare automaticky zablokovala dosud největší zaznamenané DDoS útoky, které dosáhly nejvyšší hodnoty 7,3 Tb za sekundu (Tbps) a 4,8 miliardy paketů za sekundu (Bpps). (Cloudflare 2025)

Oproti klasickému útoku DoS, který je veden z jediného zdroje, DDoS využívají více vzdálených systémů (tzv. botnetů) k současnému masivnímu útoku na cílený zdroj. Botnety, které se stále častěji využívají nejen k DDoS útokům, ale také k neviditelné a distribuované exfiltraci citlivých dat, jsou velké sbírky zombie počítačů (bots), které jsou řízeny skrze bot herder. Vzhledem k tomu, že útok může pocházet ze stovek až tisíců počítačů, není možné jej zastavit pouhým zablokováním jedné IP adresy. (Brooks et al. 2018).

**Botnet**

V odborné studii Method and Means of Critical Information Processing in Corporate Networks se uvádí, že kolem 25 % incidentů úniků dat v korporátním sektoru jsou následkem aktivity botnet. (Huralnyk et al. 2025) Botnet je rozsáhlá síť kompromitovaných zařízení nazývaných boti nebo zombie, která je řízena skrze bot herder. Tyto sítě mohou obsahovat i miliony koncových zařízeních, jejichž majitelé netuší, že jsou infikována. Botnet je zneužívaný například k útokům typu DoS/DDoS (Brooks et al. 2018) nebo prohledávání a krádeži citlivých dat, tj. exfiltraci dat.

**Sociální inženýrství**

Protože se technická opatření ve firmách stále zlepšují, zaměřují se útočníci na lidský faktor, který je často považován za nejslabší článek bezpečnostního perimetru. (Verizon 2022) Cílem sociálního inženýrství je zneužít lidskou důvěřivost a skrze psychologickou manipulaci získat citlivé údaje, které mohou sloužit například k neoprávněnému vstupu do interní sítě podniku.

Podle studie z roku 2022 přicházejí podniky při útocích skrze sociální inženýrství průměrně o 130000 dolarů. (Burge et al. 2022) Nejlepší způsob, jak tomuto typu útoku předejít, je zavedení firemní politiky, která plošně zakazuje zasílání citlivých informací mimo interní síť podniku. Klíčové je i vzdělávání zaměstnanců v oblasti kyberbezpečnosti. (Brooks et al. 2018).

Protože sociální inženýrství z principu vyžaduje spolupráci své oběti, stávají se z uživatelů interních podnikových sítí nechtění spolupachatelé. V takových případech nejde tedy pouze o hrozby od externích aktérů, ale i těch interních.

## INTERNÍ AKTÉŘI

Interní hrozby (Insider Threat) jsou jeden z nejzávažnějších faktorů ohrožujících důvěrnost a integritu dat v moderních organizacích. (De Sousa a Shahzad 2021) Interní hrozbou se rozumí riziko pocházející od jednotlivců, kteří mají legitimní přístup k síti, systémům nebo datům společnosti, například protože jsou současnými nebo bývalými

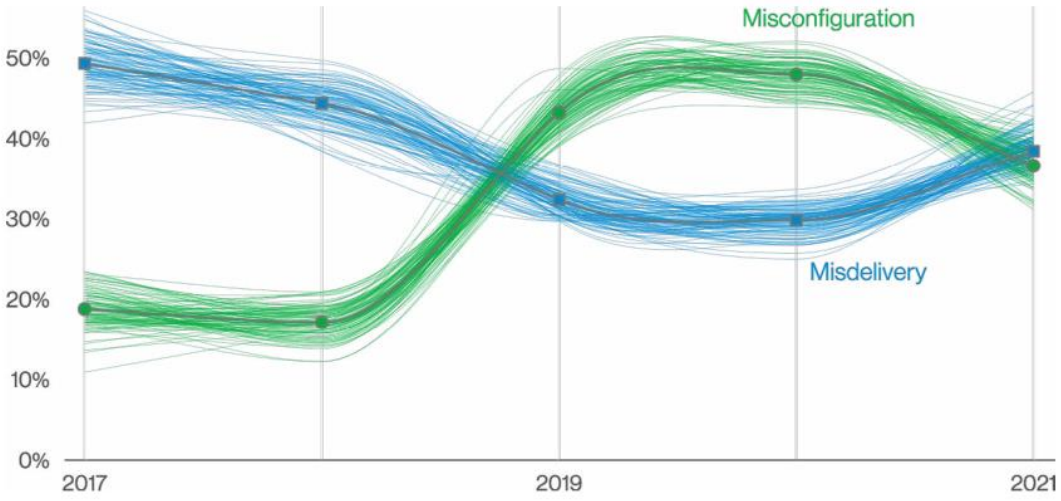
zaměstnanci. Tito aktéři – zaměstnanci, dodavatelé nebo třeba obchodní partneři – mohou ohrozit integritu dat, finanční stabilitu i reputaci podniku. Důležité je i to, že riziko se týká nejen standardních zaměstnanců, ale i privilegovaných uživatelů, jako jsou IT administrátoři nebo vedoucí pracovníci, kteří disponují vysokou úrovní oprávnění s přístupem k rozsáhlým aktivům.

Podle výsledků studií jsou interní aktéři zdrojem až 20 % bezpečnostních incidentů v podnicích (Verizon 2022) a tyto incidenty mívají častěji závažnější důsledky než incidenty externí. Historická data ukazují, že medián množství kompromitovaných záznamů následkem bezpečnostní události způsobené interním aktérem překonal ten externí více než desetkrát. (Verizon 2008)

Vnitřní hrozby se obecně dají rozdělit na úmyslné a neúmyslné jednání interních aktérů.

Koncept úmyslného zneužívání legitimních přístupu k datům se někdy nazývá termínem "Malicious Insider" neboli zlomyslný interní pracovník. Motivace k úmyslnému vynesení dat mohou být různé, nemusí jít pouze o finanční zisk ale i například o mstu zaměstnavateli nebo ideologické či politické přesvědčení.

Úniky dat způsobené neúmyslně jsou nejčastěji následkem nedbalosti osob. Interní aktéři mnohem pravděpodobněji (až sedmkrát častěji) způsobí chybu, která vede k nežádoucí manipulaci s daty, než že by únik způsobili úmyslně. Významnými typy neúmyslného úniku jsou Nesprávné nastavení (Misconfiguration) a nesprávné odeslání (Misdelivery). Právě nesprávné nastavení sleduje od roku 2018 vzrůstající trend, jak je vidět v grafu 2. To je spojené především s nárůstem využití cloudových uložišť, která často nemají vhodně nastavena přístupová oprávnění. (Verizon 2022)




*Graf 2 - Bezpečnostní incidenty způsobené neúmyslným chováním interních aktérů*

*Zdroj: (Verizon 2022)*

### 3.1.2 Normy a standardy

Organizace po celém světě používají mezinárodní technické standardy pro vytvoření, implementaci, udržování a vylepšování komplexních bezpečnostních systémů. (Brooks et al. 2018) Rámce jako NIST Cybersecurity Framework a ISO/IEC 27001 jsou dobrovolné, ale důležité, protože poskytují organizacím nezbytnou strukturu pro řízení informační bezpečnosti. Namísto ad-hoc bezpečnostních opatření nabízí tyto standardy systematický a opakovatelný přístup k zajištění bezpečnosti.

**ISO/IEC 27001**

Tato norma je celosvětově nejznámějším standardem pro systémy řízení informační bezpečnosti neboli ISMS. ISO 27001 je vodítkem, jak nastavit řádné ISMS ve firmách všech velikostí a ze všech odvětví. (Kyriazoglou 2024) Soulad s touto normou prokazuje, že organizace efektivně řídí rizika související se zabezpečením dat v souladu s mezinárodními osvědčenými postupy. Bezpečnostní opatření dle ISO 27001 se dotýkají čtyř úrovní:

- Organizační (např. bezpečnostní politiky)
- Lidské (např. vzdělávání zaměstnanců)
- Fyzické (např. fyzické kontroly vstupů)
- Technologické (např. šifrování dat nebo firewall)

**NIST Cybersecurity Framework**

Tento rámec byl vyvinut americkým Národním institutem pro standardy a technologie. Skládá se z řady pokynů k implementaci a modernizaci kyberbezpečnostních systémů, které nejsou vázané na žádný konkrétní produkt a díky tomu jsou přizpůsobitelné potřebám každé organizace. (Brooks et al. 2018) V rámci tohoto standardu je kybernetická bezpečnost rozdělena na 5 základních funkcí:

- **Identifikace:** Identifikací je myšleno porozumění tomu, jakými aktivy firma disponuje, jaká zpracovává data, jaké využívá systémy atd. K tomu se vztahuje i prioritizace zdrojů podle toho, jak jsou klasifikovány.
- **Ochrana**: Cílem této funkce je chránit integritu, důvěrnost a dostupnost informací. Patří sem například řízení identit a přístupů, ale i školení zaměstnanců v oblasti kyberbezpečnosti.
- **Detekce:** Detekce se vztahuje k včasnému zjištění výskytu bezpečnostní události. Podle studie z roku 2022 trvalo podnikům v průměru 277 dní, než zjistily, že došlo k narušení ochrany dat. (IBM Corporation 2022) Monitorování systémů, sítě i fyzického prostředí je proto jedním ze základních pilířů kyberbezpečnosti.
- **Reakce**: V návaznosti na včasnou detekci je nutné i neodkladné řešení incidentu. Reakce se zaměřuje nejen na provedení opatření, ale i na pochopení záchytu a omezení vzniku dalších incidentů.

- **Obnova** – Pro případ, že následkem bezpečnostního incidentu dojde k narušení některých provozních funkcí, musí mít firma připravený plán obnovy. Součástí něj je i řízení vztahů s veřejností.

### 3.1.3 Legislativní požadavky v EU a ČR

Kromě norem a standardů, jejichž aplikace je nepovinná, existují i regionální zákony a regulace, které pro podniky stanovují bezpečnostní povinnosti. Jejich cílem je zajistit, aby firmy adekvátně investovaly do ochrany dat. V případě nedodržování těchto právních závazků hrozí firmám regulatorní sankce.

**Směrnice NIS 2**

Směrnice NIS 2 reviduje směrnici (EU) 2016/1148 o bezpečnosti sítí a informačních systémů (Network and Information Security, NIS) s cílem dosáhnout vysoké společné úrovně kybernetické bezpečnosti v celé EU. (European Commission 2025) Zaměřuje se na 18 kritických sektorů napříč členskými státy, např. zdravotnictví, energie, veřejná správa atd. Zpravidla dopadá na střední a velké podniky, ale státy do ní mohou zařadit i menší organizace s vysokým rizikem. Subjekty se dělí na zásadní (essential) a důležité (important) s rozdílným režimem dohledu a výši sankcí.

Pro obě kategorie platí, že je u nich nutné zavést řízení kybernetických rizik, a to minimálně v rozsahu následujícího desatera (The NIS2 Directive 2023):

1. politiky řízení rizik a bezpečnosti IS
2. řízení incidentů
3. řízení kontinuity podniku + krizové řízení
4. bezpečnost dodavatelského řetězce
5. bezpečnost při pořizování, vývoji a údržbě systémů
6. postupy pro hodnocení účinnosti opatření
7. základy kybernetické "hygieny" a školení
8. politiky využívání kryptografie a šifrování
9. personální bezpečnost a řízení přístupů
10. využívání vícefaktorového ověřování a zabezpečené komunikace

Zároveň vzniká pro podniky povinnost hlášení významných bezpečnostních incidentů do 72 hodin od jejich vzniku. Celkově směrnice klade důraz na spolupráci, jak v rámci dodavatelského řetězce a s příjemci služeb, tak i s orgány dohledu, které mohou provádět v organizacích on-site i off-site audity. Do českého právního řádu se směrnice implementovala skrze nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti, s účinností od 1.11.2025.

Nedodržováním tohoto předpisu a povinností z něj vyplývajících se podniky vystavují riziku sankcí (European Commission 2025):

a) až 10 milionů Euro nebo 2 % ročního obratu pro zásadní subjekty,
b) až 7 milionů Euro nebo 1,4 % ročního obratu pro důležité subjekty.

**EU Cyber Acts**

Cybersecurity Act, Cyber Resilience Act a Cyber Solidarity Act se jako evropská nařízení vzájemně doplňují a společně mají za cíl nastavit jednotný rámec kybernetické bezpečnosti napříč členskými státy v oblastech od vývoje, poskytování a certifikace produktů i služeb až po soudržnost při společných reakcích na bezpečnostní incidenty. Vzhledem k zvyšujícím se rizikům je kladen velký důraz na budování odolnosti a důvěry a odstranění roztříštěnosti trhu.

**eIDAS 2**

IDAS 2 je zkratka pro nařízení (EU) 2024/1183, které novelizuje původní eIDAS (č. 910/2014) a zřizuje Evropský rámec digitální identity. Cílem je zajistit bezpečnou a právně uznávanou elektronickou identifikaci a důvěryhodné služby vůči veřejné správě i v soukromém sektoru. Klíčovým prvkem je vytvoření a řízení obecně uznávané European Digital Identity (EUDI) Walletu, tedy „peněženky" pro ukládání a prokazování totožnosti. (Kovář a Amler 2021)

**GDPR**

GDPR neboli nařízení 2016/679 Sb., o ochraně osobních údajů je evropská regulace, která představuje pro fyzické osoby velký převrat v oblasti ochrany jejich osobních údajů. Do roku 2018, než vzešlo nařízení v účinnost, byla pravidla k ochraně osobních dat napříč EU nejednotná a často nedostačující. (Ruohonen et al. 2021)

S vzestupem digitálních médií se osobní údaje staly čím dál tím víc žádanější komoditou a i legitimní podniky měly (a někde i stále mají) tendenci shromažďovat jich co nejvíce, buď pro svou vlastní potřebu nebo k prodeji třetím stranám. Následkem úniků dat z těchto platforem se osobní údaje často ocitají na černém trhu. Účet ze sociální sítě Facebook, který obvykle obsahuje obrovské množství soukromých informací, se na dark webu prodává za cca 50 dolarů a kompletní zdravotní údaje mohou být oceněny až na více jak 500 dolarů. (Khalil 2025) GDPR mělo a má za cíl navrátit fyzickým osobám kontrolu nad jejich osobními daty a najít vhodný kompromis k dosažení regulovaného prostředí pro mezinárodní obchod napříč EU. (Kyriazoglou 2024) Důležitý je i fakt, že bez ohledu na to, kde jsou data zpracovávána, pokud byla shromážděna v EU, vztahuje se na ně GDPR.

GDPR je postaveno na několika základních principech:

- **Zákonnost, korektnost a transparentnost:** Zpracování musí probíhat v souladu s právními předpisy, s férovým přístupem k subjektům, jejichž data se zpracovávají, a za jejich informovanosti.
- **Omezení účelů, kdy je možné data zpracovávat**: Data lze zpracovávat pouze pokud pro to existuje výslovně stanovený legitimní účel.
- **Minimalizace dat:** Je možné zpracovávat pouze takový rozsah dat, který je nezbytně nutný pro dosažení daného účelu

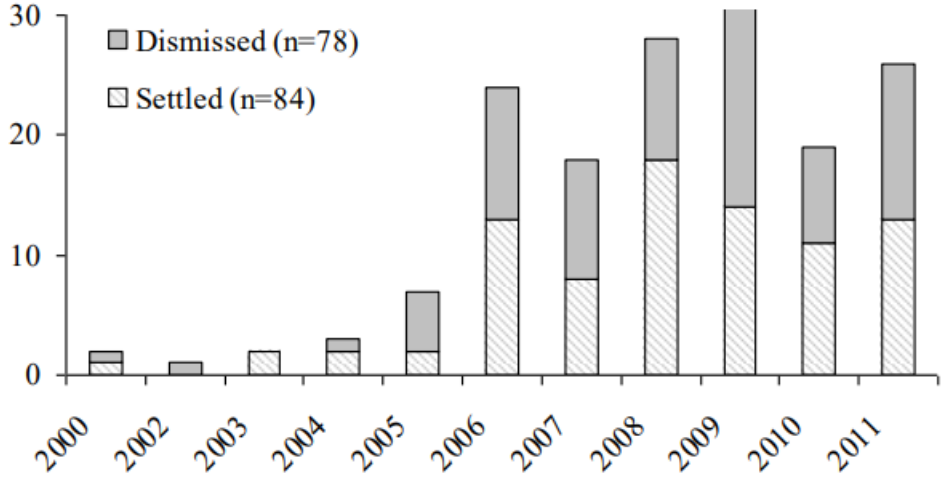
### 3.1.4 Dopady kybernetických útoků

Vzhledem k rozsahu informací, které firmy v dnešní době obvykle zpracovávají, mohou být úniky dat jednou z nejzávažnějších bezpečnostních situací, s kterou se podniky setkávají. Z nenápadné bezpečnostní slabiny se velmi rychle může stát celopodniková krize, s významnými následky. (Kyriazoglou 2024) Kromě finančních škod představují kybernetické útoky také hrozbu pro reputaci firmy, což může vést ke ztrátě důvěry zákazníků i obchodních příležitostí. Obecně lze dopady úspěšného kybernetického útoku dělit na přímé a nepřímé.

a) **Přímé následky** mají obvykle finanční charakter, jsou nejlépe viditelné a kvantifikovatelné. Nejčastěji se jedná o *regulační pokuty a sankce* udělené následkem nedodržování stanovených předpisů k ochraně dat. Jak již bylo zmíněno výše, v případě NIS 2 nebo GDPR se může za určitých podmínek jednat až o procenta celoročního obratu. Z výzkumů vyplývá, že pro třetinu postižených firem byly pokuty natolik významné, že poškodily jejich finanční zdraví. (Hiscox 2025)

   Úniky dat také často vedou k hromadným žalobám ze strany poškozených jednotlivců, kteří požadují *právní náhradu za škody* způsobené ztrátou nebo krádeží jejich osobních údajů. Pravděpodobnost, že firma bude žalována, je 3,5krát vyšší, pokud jednotlivci utrpí prokazatelnou finanční újmu (Romanosky et al. 2014)

   Mimo regulační pokuty a soudní spory patří mezi přímé dopady i *náklady na nápravu a likvidaci incidentu* – forenzní analýzu, obnovu systémů, implementaci nových procesů atd. Někdy musí podniky zvážit i *náklady spojené s notifikací zákazníků* o úniku jejich dat. Z některých zdrojů vyplývá, že průměrné celkové náklady na únik dat činí až 4,88 milionu USD (Bartley 2025).




*Graf 3 - Vyřešené a zamítnuté soudní spory týkající se porušení ochrany osobních údajů v letech 2000 až 2011*

*Zdroj: (Romanosky et al. 2014)*

b) **Nepřímé následky** jsou často dlouhodobé a ovlivňují vztahy se zákazníky a důvěru v organizaci. Tyto dopady obvykle nelze jednoznačně kvantifikovat, ale narušení očekávání zákazníků, že jejich data budou dostatečně chráněna, vede k prokazatelnému snížení důvěry ve společnost. (Markos 2023) Ztráta určitých typů dat, jako jsou informace o platebních kartách nebo rodné číslo, má negativní a statisticky významný dopad na ochotu spotřebitelů pokračovat v obchodních vztazích s danou organizací. Zaměstnanci postižených firem navíc čelí obrovskému stresu, což může vést ke zvýšené absenci nebo syndromu vyhoření. (Hiscox 2025)

### 3.1.5 Architektura bezpečnostních systémů podniku a standardní nástroje

V rámci ochrany informací je důležitá nejen kybernetická ochrana, ale i ta fyzická. V knize Cybersecurity Essentials uvádí autor, že "bez fyzické bezpečnosti neexistuje žádná bezpečnost" a "veškerá bezpečnost začíná na úrovni fyzického přístupu" (Brooks et al. 2018). V tomto pojetí pod sebou tedy kybernetická ochrana zahrnuje nejen zajištění nehmotných aktiv (dat, softwaru, duševního vlastnictví), ale i zajištění fyzického přístupu k systémům a koncovým zařízením. Výzkum se dnes zaměřuje už i na dosud podceňované zranitelnosti na síťové a fyzické úrovni jako například elektromagnetické úniky skrze hardware (Sachenko et al. 2025).

Architekturu bezpečnosti lze z mnoha pohledů popsat stupňovitým přístupem nebo přesněji topologií bezpečnostních vrstev, které tvoří tři základní složky, kde každá z nich zahrnuje své vnitřní perimetry ochrany. (Brooks et al. 2018) Konkrétně jde o složky:

- Zabezpečení pozemků a budov (fyzická ochrana nemovitého majetku)
- Zabezpečení koncových zařízení a dat, které se na nich nacházejí (fyzická ochrana movitého majetku a částečně i kybernetická ochrana)
- Zabezpečení informací v rámci síťového perimetru (kybernetická či logická ochrana)

Každá složka má svých několik vrstev, které definují. V rámci fyzické ochrany jde o:

1. Vnější perimetr, který slouží jako první linie obrany. Obvykle se jedná o vymezenou hranici pozemku nebo vnější stěny budovy podniku.
2. Vnitřní perimetr, který zahrnuje bariéry uvnitř budovy, například stěny, dveře, okna atd., které brání vstupu do kritických oblastí budov, kde se nachází cenná aktiva společnosti.
3. Interiér, jež je nejvíce zanořenou vrstvou, jedná se o ochranné "schránky", kde se aktiva nachází. Může to být trezor nebo zamčená skřínka s dokumenty ale také třeba celá serverovna.

Obdobným způsobem se dá nahlížet i na zabezpečení endpointů neboli koncových zařízení:

1. Vnější perimetr je fyzická schránka koncového zařízení
2. Vnitřní perimetr je tvořen operačním systémem a aplikacemi
3. Interiér jsou samotná nehmotná data, tj. soubory a složky

Síťový perimetr primárně tvoří hranice mezi privátní sítí (intranetem), kde má podnik stále plnou kontrolu nad pohybem dat, a veřejnou sítí (internetem), kam už podnik může zasahovat pouze omezenými prostředky. V tomto místě jsou obvykle implementovány zabezpečovací prvky, které chrání před vnějšími kybernetickými hrozbami.

**Firewall**

Firewall je často první linií obrany sítě připojené k internetu. (Brooks et al. 2018) Základy k jejímu vzniku byly položeny už v 80. letech 20. století a přestože od té doby prošla rozsáhlým vývojem, je stále nejužívanějším nástrojem kybernetické bezpečnosti jak v podnicích tak na soukromých zařízeních.

Firewall typicky definuje bezpečnostní perimetr, tedy hranici, kde se soukromá síť setkává s vnější sítí (internetem) a kde má firma stále ještě kontrolu nad síťovým provozem. Jak už vyplývá z jejího názvu, jde o bariéru, která filtruje datové pakety a kontroluje tok informací mezi vnitřním a vnějším prostředím. (Iavich et al. 2024) Tímto způsobem brání neoprávněnému přístupu do důvěryhodného interního prostředí nebo zanesení jakéhokoliv typu malwaru do koncového zařízení.

Obdobně jako ostatní bezpečnostní softwary lze firewall klasifikovat podle typu implementaci na hardwarový (síťový) firewall a softwarový (hostitelský) firewall. (Brooks et al. 2018) Hardwarová firewall může být vestavěna přímo do routeru nebo přepínače a umožňuje správci kontrolovat tok informací ke všem zařízením připojeným do sítě. Softwarový firewall je implementován jako běžná aplikace na koncovém zařízení. Většina dnešních moderních zařízení, které umožňují přístup na internet, už dnes mají předem vestavěnou softwarovou firewall. Tyto řešení chrání lokálně jednotlivé zařízení.

Firewall pracuje s definovanými pravidly, podle kterých se rozhoduje, zda přijmout nebo odmítnout příchozí i odchozí datové pakety, a to na základě jejich adres, logických portů nebo protokolů. (Iavich et al. 2024) Tento proces se nazývá filtrování paketů (packet filtering) a může se dělit na filtrování bezespojové (statické) a spojové (stavové). (Brooks et al. 2018) Pokročilými funkcemi firewall může být jejich integrace s Proxy servery, kdy dochází ke komplexnějšímu filtrování dat, což je sice pomalejší ale zároveň bezpečnější způsob ochrany.

Pro integraci firewall s dalšími bezpečnostními systémy je také důležité znát její typ (Skrunda 2025):

- **Firewally s filtrováním paketů:** Tyto firewally zkoumají jednotlivé datové pakety. Na základě předem definovaných pravidel týkajících se IP adres, čísel portů a protokolů pakety povolují nebo blokují. Jsou sice účinné, ale mohou postrádat pokročilé bezpečnostní funkce.

- **Firewally se stavovou kontrolou:** Na rozdíl od firewallů s filtrováním paketů udržují firewally se stavovou kontrolou stavovou tabulku aktivních připojení. To jim umožňuje sledovat stav síťových připojení a činit informovanější rozhodnutí o povolení nebo blokování provozu.
- **Firewally nové generace (NGFW):** NGFW integrují tradiční funkce firewallu s pokročilými schopnostmi, včetně prevence narušení, rozpoznávání aplikací a hloubkové kontroly paketů. Tato kombinace zvyšuje bezpečnost proti současným hrozbám.
- **Firewally webových aplikací (WAF):** WAF se zaměřují na ochranu webových aplikací monitorováním a filtrováním HTTP provozu. Zaměřují se konkrétně na webové útoky, jako je cross-site scripting (XSS) a SQL injection.

**IDPS**

Jedny z nejzákladnějších systémů pro zajištění kybernetické bezpečnosti podnikové IT infrastruktury jsou systémy detekce průniku IDS (Intrusion Detection Systems) a systémy prevence průniku IPS (Intrusion Prevention Systems), někdy souhrnně označované jako IDPS. Jejich hlavním cílem je monitorovat síťovou infrastrukturu podniku a odhalit případný neautorizovaný přístup nebo obdobnou podezřelou aktivitu. (Muhammad et al. 2023)

První výzkumné modely se objevily už v 80. letech 20. století a počátkem 21. století se v reakci na nové hrozby jako SQL injections a cross site scripting (XSS) dostali mezi best practice kybernetické bezpečnosti. (Secureworks 2024)

Systémy IDS slouží jako senzor k zachycení toku síťového provozu. Jsou to pasivní detekční mechanismy, které nahlašují incidenty, porušení bezpečnostních politik nebo neobvyklé chování v rámci sítě či systému, ale nepodnikají žádné aktivní kroky k zastavení hrozby nebo nápravě. IPS řešení navíc využívají aktivní prvky, které se snaží bránit dokončení detekovaného pokusu o průnik, a poskytují tak i automatizovanou ochranu. To umožňuje reagovat dříve, než dojde ke kompromitaci dat nebo narušení integrity systému.

Podle toho, jak jsou IDPS implementována je lze dělit na:

1. HIDS - Systémy pro detekci a prevenci průniku na bázi hostitele se instalují přímo na koncová zařízení, tj. na hostitele, a monitorují aktivity, jako jsou spouštění procesů, síťová spojení a manipulace se soubory.
2. NIDS - Network IDS: Řešení na bázi sítě monitorují primárně síťový provoz a analyzují aktivitu v síti.

Kombinací obou typů implementace je zajištěna nejefektivnější ochrana ve formě distribuovaného IDS systému.

Metody detekce (Brooks et al. 2018):

1. **Signature based detection:** Tato metoda je nejčastěji využívána jak IDPS systémy tak i například systémy SIEM a DLP. Systém porovnává síťový příchozí i odchozí provoz s databází známých vzorců útoků a pokud narazí na shodu, alertuje uživatele.

Jde o účinnou metodu při odhalování známých útoků, ale v dnešní době je nedostačující, vzhledem k neustálému rozvoji malware a dalších škodlivých aktivit.

2. **Anomaly based detection:** Pomocí statistické analýzy nebo strojového učení se vytváří tzv. baseline neboli základní profil normální provozu. IDPS pak sleduje události, které se od běžného toku dat významně odchylují a označuje je jako potencionální hrozby. Tato metoda je účinná především na zero-day útoky.
3. **Behavioral analysis (UEBA):** Spíše než o samostatnou metodu jde o směr vývoje IDPS systémů, který využívá moderní techniky strojového učení a umělou inteligenci k vylepšování detekčních schopností. Často kombinuje metody detekce založené na signaturách i anomáliích a rozšiřuje je o znalosti získané z analýzy chování systémů.

**Antivirové (antimalware) programy**

Antivirové (AV) programy jsou ochranný software, který se snaží zabránit spuštění škodlivého kódu. Viry jsou podmnožinou celkové skupiny malware a kromě nich jsou podstatné i hrozby jako trojské koně, červi nebo spyware. Proto se dnes často mluví i o "antimalware" programech. Antivirus tradičně cílí především na klasické viry a starší typy škodlivého kódu, zatímco antimalware se soustředí i na více sofistikovaná rizika (ransomware, spyware, rootkit). Oba typy softwaru jsou v praxi běžně kombinované do jednoho bezpečnostního balíku, který je poskytován uživatelům koncových zařízení. (GeeksforGeeks 2025)

Antivirové (antimalware) programy se v mnohém liší podle svého poskytovatele, ale existují vlastnosti, které jsou jim společné. Mezi ně patří:

- schopnost skenovat komprimované soubory a zabalené spustitelné soubory
- nástroje na skenování souborů a adresářů na žádost uživatele nebo nepřetržitě v reálném čase
- ovladač, který slouží k ochraně sama sebe, tj. ochraně samotného antiviru před napadením
- funkce ke kontrole síťového provozu a firewall
- grafické rozhraní a/nebo příkazový řádek
- daemon nebo služba
- řídící konzole

Jádrem antivirových produktů je interní engine, známý také jako kernel, který propojuje všechny komponenty AV. Například antivirové skenery používají API exportované jádrem k analýze souborů a adresářů. (Koret and Bachaalany 2015) Na úrovni tohoto enginu dochází k filtrování a detekci, např. před každým spuštěním souboru je požadavek na jeho otevření pozastaven, obsah je předán detekčnímu enginu a teprve podle výsledku skenu je operace povolena nebo zablokována. Část výrobců včetně Microsoft se kvůli riziku chyb v kernelu přesouvá k modelu, kde AV běží mimo jádro a používají bezpečnější systémové API. (Warren 2025)

**Šifrovací nástroje**

Jedná se o programy nebo systémové funkce, které chrání data tím, že je převádí do nečitelné šifrované podoby a poskytují klíč, kterým je lze obnovit do původního prostého textu. Postavené jsou na kryptografických algoritmech, nejčastěji na symetrickém šifrování, které využívá stejný klíč pro zašifrování i dešifrování, a na bezpečnějším asymetrickém šifrování, které využívá klíče dva (veřejný a soukromý). (Cloudflare 2025)

Dvěma významnými skupinami jsou:

- **Šifrování komunikace:** Příkladem je TLS používané na webu, které kombinuje symetrické a asymetrické šifrování a výsledkem jsou data chráněná před odposlechem a manipulací v rámci přenosu.
- **Šifrování dat v klidu** (data at rest): Jde o šifrování informací uložených na uložištích jako disk, SSD, USB atd. Nejčastější formou je full-disk encryption (FDE) neboli šifrování celého disku na úrovni blokového zařízení, kdy se mezi souborový systém a fyzické uložiště vloží šifrovací vrstva. Bez odemčení pak médium vypadá pouze jako náhodný šum.

## 3.2 DLP systémy

"DLP systém je sada nástrojů a procesů zaměřených na detekování, monitoring a ochranu citlivých dat před neoprávněným přístupem, únikem nebo krádeží" (Huralnyk et al. 2025)

Tyto systémy fungují na principu implementace jednotlivě konfigurovaných bezpečnostních politik, které naplňují základní bezpečnostní požadavky organizace. DLP řešení skrze tyto bezpečnostní politiky provádí hloubkovou analýzu obsahu a kontextu dat pohybujících se v IT infrastruktuře podniku a pomocí komplexních detekčních metod vyhledává potencionální rizika pro bezpečnost firemních informací.

Tok dat je DLP systémy nejen monitorován, ale i řízen, což zajišťuje, že nedojde k nechtěnému přesunutí dat (například odesláním nebo stažením) mimo chráněný perimetr firmy a do rukou neoprávněných osob. (Faiz et al. 2019) Moderní DLP řešení umí kromě detekce hrozeb i šifrovat data, zasílat notifikace směrem k autorizovaným složkám a blokovat uskutečnění rizikové manipulace s daty.

### 3.2.1 Klasifikace dat

Data, která jsou DLP systémy, ale i dalším bezpečnostním softwarem, chráněna se dělí do kategorií podle stavu a fáze životního cyklu, kde se zrovna nacházejí:

- **Data at Rest** – Tento stav zahrnuje data, která jsou uložena v trvalých uložištích, jako jsou databáze, cloudové a souborové servery i místní síťové disky. I když jsou data v tomto stavu považována za více zabezpečená než v dalších stavech (Faiz et al. 2019), DLP i tak monitoruje tato uložiště a proaktivně je chrání před neoprávněnou manipulací.
- **Data in Motion** – Jedná se o data, která jsou přenášena soukromou nebo veřejnou (interní nebo externí) sítí z jednoho uzlu do druhého, obvykle

prostřednictvím webových kanálů, FTP nebo e-mailu. (Huralnyk et al. 2025) DLP kontroluje tyto přenosy a komunikaci, aby zabránilo neoprávněnému nebo neúmyslnému úniku informací. Z praxe vyplývá, že právě e-mailová komunikace je často největším zdrojem rizik pro bezpečnost dat.

- **Data in Use** – Ochrana se zaměřuje na data, se kterými uživatel aktivně pracuje na svých koncových zařízeních (PC, notebook, telefon, tablet apod.). To zahrnuje monitorování a řízení práce s texty, dokumenty a aplikacemi (Faiz et al. 2019). Tímto způsobem je možné kontrolovat činnosti jako kopírování a vkládání textů, tisk dokumentů, vytváření snímků obrazovky, otevírání nebo ukládání souborů atd.

### 3.2.2 Klasifikace DLP systémů

Základní dělení architektur DLP systémů se zaměřuje na to, kde probíhá sběr událostí, analýza a správa bezpečnostních politik. DLP řešení se tak klasifikují podle modelu nasazení na centralizované, distribuované a hybridní modely, které se liší podle způsobu správy, škálovatelností a výkonem. Podrobnosti k architektuře a odlišnostem jsou uvedeny v tabulce 1.

| Model | Centralizovaný | Distribuovaný | Hybridní |
|---|---|---|---|
| **Architektura** | Veškerá logika soustředěná v jediném uzlu, obvykle v centrálním serveru, kde probíhá všechna správa politik, konfigurace a analýza událostí. | Každý uzel má své vlastní lokální analytické a rozhodovací moduly, které mohou vzájemně komunikovat | Kombinace centralizovaného řídicího serveru a více lokálních uzlů |
| **Správa** | Centralizovaná kontrola s jednodušším a rychlejším nasazením. | Složité na správu a synchronizaci bezpečnostních politik, což vede k vyšším nákladům za údržbu | Centrální server distribuuje hlavní bezpečnostní politiky, které je ale možné jemně doladit na lokální úrovni. |
| **Škálovatelnost** | Limitovaná výkonem centrální konzole. | Vysoká škálovatelnost díky automatickému zvýšení výpočetních zdrojů při přidání uzlu. | Celková flexibilita díky vertikální škálovatelnosti centrální konzole a horizontální škálovatelnosti lokálních uzlů. |
| **Výkon** | Velká zátěž na centrální uzel. Vzniká zde jednotný bod selhání, což v případě výpadku může ochromit celý systém DLP. | Vysoký výkon díky paralelnímu zpracování dat se sníženou zátěží centrálních uzlů | Část zpracování dat probíhá centrálně a část na lokálních uzlech, čímž je výkon vyvážený |

*Tabulka 1 - Klasifikace DLP systémů podle modelu nasazení*

*Zdroj: Vlastní zpracování dle (Huralnyk et al. 2025)*

DLP řešení je možné taktéž kategorizovat podle toho, kde jsou jako program nasazeny a zároveň jaký stav dat monitorují, jak je shrnuto v tabulce 2. Dělí se pak primárně na

Endpoint DLP (na koncových zařízeních) a Network DLP (síťové) a někdy také na Discovery DLP (na datových uložištích) a Cloud DLP.

| Typ DLP | Stav dat | Místo nasazení | Cílová aktivita |
|---|---|---|---|
| **Endpoint DLP** | Data in Use | Lokální koncové zařízení | Monitoruje a řídí aktivity uživatelů, jako je kopírování na externí média (USB), tisk dokumentů, používání schránky a snímání obrazovky. |
| **Network DLP** | Data in Motion | Síťové senzory, proxy, brány | Zachytává a analyzuje síťový provoz (HTTP, HTTPS, FTP, e-mail), aby zabránil neautorizovanému přenosu citlivých dat mimo síť. |
| **Discovery DLP** | Data at Rest | Datové repozitáře, souborové servery, databáze | Skenuje úložiště dat za účelem identifikace, klasifikace a označení citlivých souborů. |
| **Cloud DLP** | Data in Motion / at Rest | Cloudové prostředí (SaaS, Office 365) | Kontroluje nahrávání a stahování dat do a z cloudových služeb |

*Tabulka 2 - Klasifikace DLP systémů podle koncepčního přístupu*

*Zdroj: Vlastní zpracování dle (Huralnyk et al. 2025)*

### 3.2.3 Procesy a metody

Způsoby, jakými DLP systémy analyzují data se dají rozdělit do dvou skupin:

**Metody založené na analýze obsahu:**

Tato skupina metod se soustředí přímo na to, co je v datech obsaženo. Patří sem například shoda klíčových slov a regulárních výrazů, kde je základním principem skenování obsahu a jeho následné porovnávání s databází klíčových slov, frází nebo regulárních výrazů. Tuto databázi vytváří a spravují metodici DLP systémů. Tímto způsobem lze sledovat manipulaci s citlivými informacemi jako jsou rodná čísla, bankovní údaje nebo zdrojový kód. (Faiz et al. 2019) Další využívanou metodou je přesná shoda dat často označována zkratkou EDM (Exact Data Matching). Ta umožňuje srovnávat přenášené informace s přesnými vzory známých dat, například šablony citlivých dokumentů.

**Metody založené na analýze kontextu:**

Tyto metody nezkoumají samotný obsah dat, ale spíše okolnosti, za jakých je s daty manipulováno, a metadata k nim připojená. V rámci kontroly kontextu se DLP zaměřuje na údaje o odesílateli a příjemci, zdroj a cíl dat, jejich formát a velikost atd.

Metody analýzy obsahu a kontextu se často vzájemně doplňují. Příkladem může být situace, kdy je bezpečnostní politika nastavena tak, aby docházelo k záchytu e-mailové komunikace, pokud a) cílem přenosu je e-mailová schránka nacházející se mimo interní síť podniku (kontextová analýza) a zároveň b) v těle nebo příloze zprávy se nachází rodná čísla (obsahová analýza). Vzniklý bezpečnostní incident zde bude výsledkem obou typů analýz.

### 3.2.4 Přehled dostupných řešení

Nabídka DLP řešení je rozsáhlá, od jednoduchých open source systémů vhodných pro menší firmy, až po komplexní soubory systémů a jejich modulů. Níže v tabulce 3 je výčet nejlépe hodnocených DLP řešení na trhu dle Gartner, Inc.

| DLP řešení | Poskytovatel | Model nasazení | Pokrytí kanálů | Podpora UEBA | Škálovatelnost |
|---|---|---|---|---|---|
| **Forcepoint DLP** | Forcepoint | On premise, cloud, hybrid | Endpoint, Network, Storage (Data at Rest), Cloud | Ano | Střední a velké podniky |
| **Cisco Umbrella** | Cisco Systems | Cloud-native SaaS | Network, Cloud | Odděleně | Univerzální |
| **Trellix Data DLP** | Trellix | On premise, cloud, hybrid | Endpoint, Network, Cloud | Odděleně | Střední a velké podniky |
| **Symantec DLP** | Broadcom | On premise, cloud, hybrid | Endpoint, Network, Storage (Data at Rest), Cloud | Ano | Velké podniky |
| **Proofpoint Enterprise DLP** | Proofpoint | Cloud-first SaaS | Endpoint, Network | Ano | Střední a velké podniky |
| **CrowdStrike Falcon** | CrowdStrike | Cloud-native SaaS | Endpoint, Cloud | Ano | Střední a velké podniky |
| **GTB Technologies DLP** | GTB Technologies | On premise, cloud, hybrid | Endpoint, Network, Storage (Data at Rest), Cloud | Ne | Střední a velké podniky |
| **Fortra's Digital Guardian** | Fortra | On premise, cloud, hybrid | Endpoint, Network, Storage (Data at Rest), Cloud | Ano | Střední a velké podniky |
| **Endpoint Protector** | Netwrix | On premise, cloud | Endpoint, Storage | Ne | Univerzální |
| **Teramind DLP** | Teramind | On premise, cloud | Endpoint, Network, Cloud | Ano | Malé a střední podniky |

*Tabulka 3 - Nejlépe hodnocené DLP systémy k roku 2025*

*Zdroj: Vlastní zpracování dle (Gartner, Inc. 2025) a stránek jednotlivých dodavatelů řešení.*

## 3.3 SIEM

Zkratka SIEM se skládá se dvou termínů:

1. Security Information Management (SIM), související se sběrem dat a reportováním nad nimi.
2. Security Event Management (SEM), ukazující na možnost reagovat na bezpečnostní incidenty v reálném čase.

Systémy SIEM se využívají k centralizované kontrole nad bezpečnostními systémy. Důvodů k jejich implementaci v podniku je hned několik:

- K ochraně před bezpečnostními hrozbami používají podniky mnoho různých softwarových nástrojů. Jejich počet se navíc časem zpravidla rozrůstá společně s tím, jak se zvyšuje množství dat zpracovávaných v čím dál více komplexním IT prostředí. Různé systémy také často běží v různých verzích a jsou aktualizovány v nesynchronizovaných termínech.

- Mnoho bezpečnostních systémů nedokáže pracovat se záchyty v reálném čase. Ze studie Verizonu 2025 Data Breach Investigation vyplývá, že nalezení a napravení slabin u zařízeních na perimetru trvá průměrně 32 dní. (Verizon 2025)
- U středně velkých až velkých firem mohou být do korporátní sítě zapojené stovky až tisíce zařízení využívaných stovkami zaměstnanců s různými úrovněmi schopností práce s technologiemi.
- Pracovníci IT a správci bezpečnostních procesů se často střídají a přináší různé pohledy na to, jak s použitým softwarem pracovat.
- Problémem jsou i sofistikované kybernetické útoky využívající vícero útočných bodů, které je těžké zachytit a řešit navzájem izolovanými systémy. (Iavich et al. 2024)

Z bodů výše vyplývá, jak komplikované je získat ucelený náhled na celou strukturu podniku a její slabiny v kontextu bezpečnostních opatření, které daná firma aplikuje.

SIEM řešení dokáže logovat a analyzovat události ze všech napojených bezpečnostních systémů. To, co se jednomu systému může zdát nepodstatné, může být v jiném systému považováno za hrozbu. Například, firewall nebude blokovat tok dat na určité IP adrese, protože nemá důvod ji považovat za rizikovou, ale v Active Directory lozích je tato IP adresa vedená jako potenciálně nebezpečná. SIEM dokáže oba toky logů zkombinovat, analyzovat a zaslat firewallu pokyn k blokaci dané IP adresy. (Podzins a Romanovs 2019)

### 3.3.1 Architektura SIEM

Architektura SIEM je založená na několika klíčových komponentách, které zpracovávají bezpečnostní události v logickém sledu, jak je zobrazeno na obrázku 1. Životní cyklus bezpečnostních událostí se někdy označuje zkratkou CAR – Collection (Sběr), Aggregation/Analysis (Agregace/Analýza), Retention (Uchování). (Chopra a Mahapatra 2019) Zdroje jako *Enhancing Security Information and Event Management to Develop Future-Ready Security Operations Center* (Raju 2016) a *Security Information and Event Management (SIEM): analysis, trends and usage in critical infrastructures* (González-Granadillo et al. 2021) uvádí, že typická SIEM infrastruktura se skládá z šesti hlavních komponent:

- Zdrojová zařízení
- Sběr logů
- Normalizace a parsování
- Moduly pravidel a korelací
- Uložiště logů
- Monitorování událostí

**Zdrojová zařízení**

Zdrojová zařízení představují primární vstupy, které komunikují se SIEM systému skrze bezpečnostní protokoly (logy). Tyto systémy jsou v podstatě senzory, které reportují bezpečnostní události napříč podnikovou infrastrukturou. Mezi tyto zdroje patří například síťová zařízení (routery), servery (aplikační, databázové, autentizační systémy), systémy obrany perimetru (firewally, IDS/IPS) a koncová zařízení - endpointy. (Bhatt et al. 2014)

**Sběr logů**

Moderní SIEM systémy jsou schopny sbírat obrovské množství dat ze stovek i tisíců zdrojů a agregovat je v reálném čase. (SentinelOne 2025). Sběr logů se často provádí pomocí specializovaných konektorů nebo agentů. Agenti jsou často instalováni na zdrojových zařízeních a běží na pozadí, kde shromažďují informace z logů a odesílají je do sběrných bodů SIEM systému, které jsou navrženy tak, aby přijímaly data v různých formátech. Existují dvě hlavní metody sběru dat: PUSH a PULL.

1. PUSH: Zdrojové zařízení proaktivně odesílá (pushing) logy do SIEM v reálném čase.
2. PULL: SIEM si data periodicky stahuje (pulling) ze zdrojového zařízení.

**Normalizace a parsování**

Vzhledem k tomu, že se logy sbírají ve specifických formátech podle dodavatele softwaru nebo typu zařízení, musí je SIEM převést do jednotného standardizovaného "tvaru". Tento proces je nezbytný, aby bylo možné provádět korelaci událostí s co největší efektivitou. Parsování navíc rozděluje data logů na strukturované prvky, což usnadňuje identifikaci a analýzu konkrétních detailů.

**Moduly pravidel a korelací**

V další fázi dochází ke zpracování normalizovaných dat. V modulu pravidel jsou uloženy všechny zásady definované administrátory, podle kterých dochází k rozhodování, zda zpracovávané logy signalizují bezpečnostní hrozbu nebo ne. Těchto pravidel pak využívá korelační modul, který se dá považovat za analytické jádro (Raju 2016) a nejdůležitější část SIEM systémů (SentinelOne 2025). Moderní SIEM systémy využívají analýzu anomálií, v rámci které se pomocí technologií strojového učení hledají vzorce chování, které se odlišují od zavedených standardů (tedy normálního chování).

**Uložiště logů**

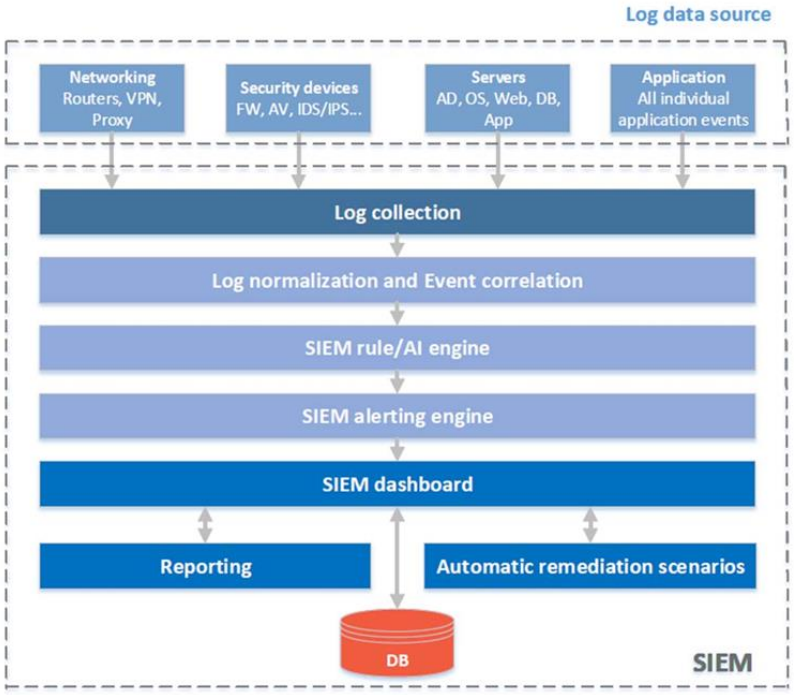
SIEM systémy mohou logy uchovávat po různě dlouhou dobu. Krátkodobé uchovávání, obvykle po dobu několika hodin, probíhá na platformě pro správu zabezpečení, kde se analyzuje okno událostí. Dlouhodobé ukládání, například kvůli další forenzní analýze dat nebo pro prokazování souladu s regulačními požadavky, je možné v archivační databázi. Zde se data mohou ukládat i několik let

**Monitorování**

Jedná se v podstatě o frontend SIEM systému (dashboard), který umožňuje analytikům v rámci Security Operations Center (SOC) aktivně sledovat události v reálném čase a dále s daty pracovat. Vizualizace logů je zásadní, protože SIEM systémy zpracovávají obrovské množství bezpečnostních dat, která by v surové formě byla pro koncové uživatele (analytiky) nesrozumitelná. Moderní SIEM systémy také umožňují customizaci dashboardů, aby bylo možné prioritizovat klíčové indikátory a bezpečnostní incidenty. (SearchInform 2025)

Dalšími SIEM komponenty jsou také prvky alertování a reportování.

- Alertování je výstupem korelačního modulu, prioritizuje se u něj rychlost a nízká míra false positive záchytů. Efektivní alertování umožňuje okamžité vyrozumění bezpečnostních týmů v případě zjištění hrozby nebo nahlášení problému, čímž se zkracuje doba potřebná k odstranění zranitelnosti. (SearchInform 2025) Alerty jsou obvykle zpracovávány analytiky SOC, kteří provádí další vyšetřování.
- SIEM zároveň generuje pravidelné reporty, které slouží k získání přehledu o celkovém stavu bezpečnosti organizace a případně k potvrzení souladu s předpisy.




*Obrázek 1 - Architektura systému SIEM*

*Zdroj: (Podzins and Romanovs 2019)*

Jednou s klíčových metrik SIEM systémů je schopnost rychle a přesně reagovat na nové i již existující hrozby. Na tuto problematiku se zaměřil i návrh nového typu SIEM architektury AMSEC (Attack Modelling and Security Evaluation Component) založený na metodách modelování kybernetických útoků. Hlavní rozdíl oproti dříve navrhovaným

přístupům spočívá v integraci několika zásadních funkcionalit do jedné komponenty, což má vést k lepším výsledkům v efektivním modelování útoků a hodnocení bezpečnosti v téměř reálném čase. (Kotenko et al. 2012)

Architektonické řešení AMSEC zahrnuje následující prvky:

- **Komplexní úložiště bezpečnostních dat**: Zajišťuje správu veškerých potřebných informací o síti, zranitelnostech systémů a hrozbách
- **Techniky generování stromů (grafů) útoků a závislostí služeb:** Využívá techniku topologické analýzy zranitelností (TVA) a zároveň zohledňuje i grafy závislostí služeb.
- **Využití tzv. anytime algoritmů:** Umožňuje analytické modelování v téměř reálném čase.
- **Kombinované využití grafů útoků a grafů závislostí služeb:** Slouží primárně pro predikci chování útočníka
- **Výpočet velkého množství bezpečnostních metrik: Zahrnuje** hodnocení dopadu útoku, efektivity reakce, potenciálu útoku a úrovně dovednosti útočníka
- **Interaktivní podpora rozhodování:** Má za cíl pomoct vybrat nejefektivnější bezpečnostní řešení s ohledem na preference uživatelů a parametry jako rizika, náklady a přínosy.

Tato architektura, v jejímž rámci byly vyvinuty softwarové prototypy, ukazuje, jak lze do systémů SIEM integrovat pokročilé analytické metody pro predikci a hodnocení složitých útočných scénářů.

### 3.3.2 Modely nasazení SIEM

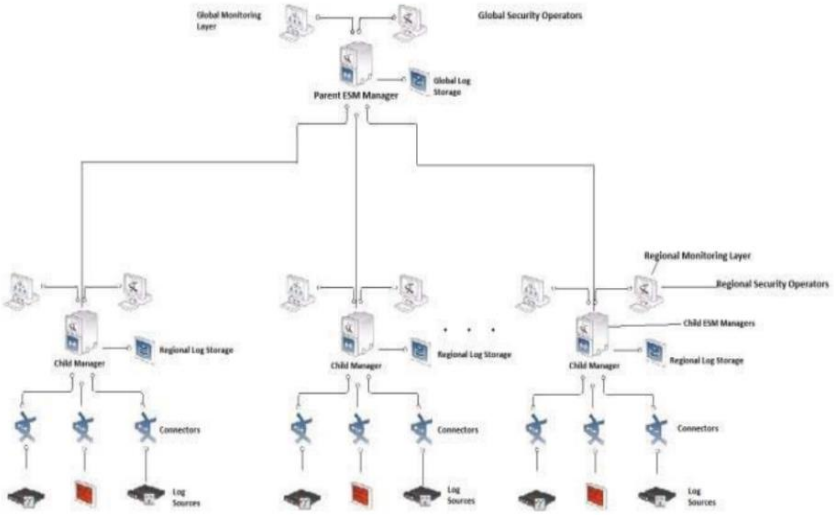
Modely nasazení SIEM systémů se dělí obdobným způsobem jako DLP řešení, a to na centralizovanou, distribuovanou a hybridní či cloudovou architekturu.

V centralizovaném modelu je veškerý sběr a analýza událostí řízen jedinou centrální konzolí, přičemž veškerá data jsou přenášena do centrálního modulu. Distribuovaná architektura provádí analýzu událostí lokálně v té části systému, kde hrozba vzniká, což snižuje zatížení centrálních uzlů. Architektury SIEM se transformovaly do cloudových nebo hybridních řešení v rámci reakce na rychlý přesun podnikových infrastruktur do cloudu. (SentinelOne 2025) Cloudové SIEM systémy se vyznačují vysokou škálovatelností, flexibilitou a jsou nákladově efektivnější, což umožňuje správu bezpečnosti napříč distribuovanými IT prostředími. Hybridní modely kombinují výhody lokálních (on-premise) řešení, zejména v rámci zachování kontroly nad citlivými daty, a zároveň nabízejí pokročilé funkce a škálovatelnost cloudových platforem.

S rostoucí velikostí podnikových sítích začali správci systémů SIEM narážet na limity ve formě nepřehledného. množství logů z obrovského množství zdrojových zařízení firmy, které se navíc lišily formáty a obsahem. K řešení problémů se škálovatelností, se kterými se

uživatelé setkávali především v centralizovaných modelech, byl navržen pokročilý typ distribuovaného modelu nazvaný Hierarchical Managers Model. (Anastasov a Davcev 2014)

Tento model, zobrazený na obrázku 2, rozšiřuje tradiční centralizovanou architekturu a zavádí hierarchii serverů. Jako centrální bod slouží Parent Node, neboli rodičovský uzel, s kterým komunikují Child Managers (podřízené servery). Ty jsou pak vázané na zdrojové zařízení. Parent Node nekomunikuje přímo se zdrojovými zařízeními a vyhýbá se zátěži spojené s prvotním zpracováním dat. Na lokální úrovni Child Managers sbírají a zpracovávají surová data, normalizují je a ukládají je na jim přidělených uložištích. Centrální úroveň pak slouží pouze pro vyšší analytické funkce jako agregace, korelace a reporting. Model doporučuje, aby i Security Operations Center byl distribuovaný obdobným způsobem na centrální a podřízené týmy.



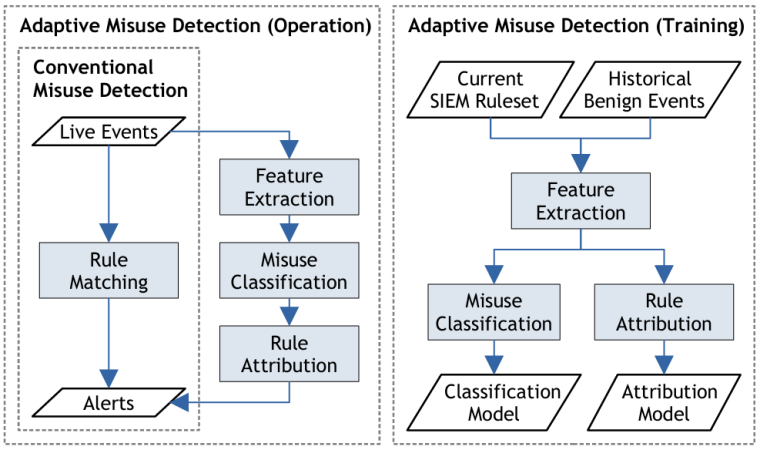

*Obrázek 2 - Architektura Hierarchical Managers modelu*

*Zdroj: (Anastasov a Davcev 2014)*

### 3.3.3 Metody detekce v SIEM

Jak bylo zmíněno, v rámci SIEM architektury se ukládají předem definovaná rozhodovací pravidla. Pravidla jsou psána experty na ochranu informací a obsahují jednu nebo více signatur, které definují, kdy se má pravidlo aktivovat. Může jít například o regulární výrazy, které porovnávají obsah podle daných vzorců. Tato metoda se nazývá detekce zneužití nebo také detekce na základě pravidel či signatur a jde o nejběžnější způsob detekce bezpečnostních událostí v SIEM systémech.

Na základě nedávné studie ale bylo zjištěno, že minimálně 44 % běžně využívaných SIEM pravidel lze jednoduše obejít. (Uetz et al. 2023). Proto byla navržena nová metoda - adaptivní detekce zneužití, která k analýze logů využívá nejen běžná pravidla, ale zároveň data srovnává se známými neškodnými událostmi. Navíc je metoda schopná detekovat, která pravidla se koncový uživatel pokusil obejít. Model této metody lze vidět na obrázku 3.




*Obrázek 3 - Model metody Adaptive Misuse Detection*

*Zdroj: (Uetz et al. 2023)*

Schopnosti systémů SIEM mohou být také rozšířeny pomocí SOAR neboli Security Orchestration, Automation, and Response. Jedná se o řešení navržené k orchestraci a automatizaci bezpečnostních systémů a tím zrychlení efektivní reakce na bezpečnostní incidenty. (González-Granadillo at al. 2021) Klíčovými složkami jsou:

- **Orchestration**: Tato složka se zaměřuje na správu pracovních toků (workflow management) a sjednocení komponent zapojených do bezpečnostních operací. Zajišťuje integraci různých bezpečnostních nástrojů, aby mohly efektivně spolupracovat.
- **Automation**: Slouží k automatizaci každodenně se opakujících procesů. Cílem je snížit potřebu manuálního zásahu lidmi, což je dnes jedním z nedostatků bezpečnostních systémů. Automatizace v kybernetické bezpečnosti může zkrátit dobu reakce na incidenty až o 85 %. (SentinelOne 2025)
- **Response**: Tato část se zaměřuje na identifikaci a řízení bezpečnostních hrozeb. Jsou v ní zahrnuty kroky, které rychle a efektivně eliminují hrozby nad rámec běžných možností systému SIEM, například okamžitá izolace napadeného endopointu.

### 3.3.4 SOC

Zkratka SOC označuje Security Operations Center neboli centrum bezpečnostních operací a v rámci podniku představuje organizační jednotku tvořenou týmem specialistů podporovaných integrovanými bezpečnostními systémy, kteří zajišťují dohled nad kybernetickou bezpečností podniku. Jejich hlavním úkolem je nepřetržitý monitoring a řízení bezpečnostních incidentů, které jsou zachytávány systémem SIEM (a dalšími bezpečnostními systémy) v reálném čase. (Podzins a Romanovs 2019) Stejně jako architektura SIEM jsou i role v SOC typicky hierarchicky strukturované podle úrovní specializace analytiků. Mimo monitorování a třídění výstrah analytici na určitých úrovních provádí i forenzní vyšetřování a spravují reakční scénáře. (Bhatt et al. 2014)

V rámci SOC probíhá reakce na incidenty dvěma způsoby: monitorováním na základě výstrah a strukturovanou reakcí na incidenty. Klasifikace rizik pak probíhá pomocí stupňovitého modelu vyšetřování (Jarrett 2025):

- Úroveň 1 (Třídění): Analytici vyřazují ze záchytů false positive výstrahy a ostatní řadí podle závažnosti.
- Úroveň 2 (Vyšetřování): Provádí se hlubší analýza s cílem získat potvrzení o skutečné hrozbě.
- Úroveň 3 (Eskalace) Potvrzené hrozby jsou eskalovány k senior analytikům, kteří incident dále řeší.

Kromě SIEM, které je považováno za vnitřní jádro architektury SOC, monitoruje operační centrum i další napojené systémy a aktiva podniku od síťové infrastruktury, firewallu, systémů pro detekci a prevenci narušení až po databázové servery a uživatelské účty. Většina podniků využívá ve svých SOC více než 25 samostatných nástrojů, včetně platforem SIEM, XDR, EDR a SOAR. (Hariharasubramanian 2025) Správně nasazený SOC představuje ucelený rámec technologií, lidí a procesů, který identifikuje, chrání, detekuje a reaguje na všechny incidenty související s bezpečností. Klíčem k úspěchu SOC jsou efektivní pracovní postupy (workflow) a správně nastavené reakce na incidenty, protože při řešení bezpečnostních záchytů může v některých případech jít o minuty nebo dokonce sekundy. (Podzins a Romanovs 2019)

V kontextu SOC funguje SIEM jako "radar" bezpečnostního týmu, jelikož testuje příchozí záznamy proti souborům pravidel a historickým datům. Mezi klíčové metriky, kterými se sleduje účinnost bezpečnostních strategií, patří (Jarrett 2025):

- **MTTR**: průměrná doba řešení incidentu od vygenerování záchytu až po vyřešení případu
- **MTTA**: průměrná doba detekce neboli doba potřebná pro klasifikaci hrozby a zahájení analýzy
- **Time to Contain**: doba zajištění aktéra a zamezení dalších vyplývajících rizik
- **False Positive Rate**: míra falešných poplachů v rámci všech záchytů
- **Event-to-Alert Time**: doba od nastání bezpečnostního incidentu po vygenerování alertu
- **Log-Source Coverage**: pokrytí zdrojů systémem SIEM
- **Quality of Investigation**: odvozená metrika ukazující, jak jsou dodržovány postupy a pokyny SOC

Nevýhody operačního centra jsou propojené s nevýhodami SIEM a nejčastější problémy spočívají v náročné a nákladné implementaci. Zároveň často dochází k zahlcení analytiků obrovským počtem záchytů, z nichž většina patří mezi falešné poplachy a je těžké z nich vyfiltrovat reálné hrozby, což snižuje efektivitu operačního týmu. Analytici, kteří třídí a klasifikují záchyty, jsou přetížení i díky náročným osmi až dvanácti hodinovým směnám včetně směn nočních, a to vede k relativně krátké době setrvání na dané pozici, často méně než dva roky. (Bhatt et al. 2014)

### 3.3.5 Přehled dostupných platforem

Stejně jako u DLP systémů je na trhu velká nabídka různorodých SIEM řešení. V tabulce 4 jsou uvedeny SIEM platformy s nejlepším uživatelským hodnocením dle Gartner, Inc, a jejich parametry.

| SIEM řešení | Poskytovael | Model nasazení | Vyhledávací jazyk | Podpora UEBA | Podpora SOAR |
|---|---|---|---|---|---|
| **Splunk Enterprise** | Cisco Systems | On-premise, Splunk Cloud (SaaS), hybridní řešení | SPL (Search Processing Language) | Splunk UBA | Splunk SOAR |
| **LogRhythm SIEM** | Exabeam | On-premise, možné v privátním i public cloudu | Lucene-based dotazovací jazyk | LogRhythm UEBA / UserXD | LogRhythm XDR |
| **IBM Security QRadar SIEM** | IBM | On-premise, QRadar Cloud (SaaS) | AQL (Ariel Query Language) | QRadar UEBA app | IBM QRadar SOAR / IBM SOAR |
| **Trellix Enterprise Security Manager** | Trellix | On-premise, možný hosting v cloudu | Proprietární Query Manager / strukturované dotazy | Fortscale UEBA / Trellix Helix | Trellix Helix |
| **Securonix Unified Defense SIEM** | Securonix | Cloud-native SaaS, hybridní řešení | Nenalezeno | vestavěné UEBA | Securonix SOAR |
| **Elastic Security** | Elastic | On-premise, Elastic Cloud (Saas) | KQL, Lucene, ES\|QL | Nenalezeno | Vestavěné i integrace s externím |
| **Logpoint - SIEM** | Logpoint | On-premise, Logpoint Cloud (SaaS) | Logpoint Query Language (vlastní syntaxe) | UEBA jako součást „Converged SIEM“ | Logpoint SOAR |
| **InsightIDR** | Rapid7 | Cloud-native SaaS | LEQL (Log Entries Query Language) | vestavěné UEBA | InsightConnect (SOAR) |
| **Falcon Next-Gen SIEM** | CrowdStrike | Cloud-native SaaS | LogScale query language | AI-driven behaviorální analytika | Falcon Fusion SOAR |
| **FortiSIEM** | Fortinet | On-premise, FortiSIEM Cloud (SaaS), hybridní řešení | FortiSIEM Query Language | behaviorální pokročilá analytika | FortiSOAR |

*Tabulka 4 - Nejlépe hodnocené SIEM systémy k roku 2025*

*Zdroj: Vlastní zpracování dle (Gartner, Inc. 2025) a stránek jednotlivých dodavatelů řešení.*

## 3.4 Integrace bezpečnostních systémů

Integrace bezpečnostních systémů mezi sebou, pro účely této práce konkrétně integrace bezpečnostních systémů jako firewall, IDS/IPS, antivirové programy atd. s centralizovanými platformami DLP a SIEM, je základním stavebním kamenem vícevrstvé kybernetické ochrany. Izolované bezpečnostní nástroje už neposkytují dostatečnou ochranu proti sofistikovaným a komplexním bezpečnostním hrozbám (Iavich et al. 2024), a proto je v dnešní době standardem vzájemně propojovat bezpečnostní prvky, tak aby došlo nejen k centralizaci řízení bezpečnosti, ale i k synergetické spolupráci mezi jednotlivými nástroji.

Důležitost integrace nástrojů bezpečnostní architektury je daná tím, jak se vzájemně doplňují. Integrace řešení pro ochranu perimetru (firewall, IDS/IPS) s ochranou endpointových bodů (antivirový software) je jedním příkladem. Důležité je i pokrytí jak ochrany toku dat (firewall), tak i kontextové ochrany obsahu (DLP). A pro dosažení komplexního přehledu o bezpečnosti podniku je nezbytné integrovat tyto systémy do centralizované platformy (DLP, SIEM), aby bylo možné rychleji a efektivněji reagovat na bezpečnostní incidenty. (SearchInform 2025)

### 3.4.1 Přenos dat mezi systémy

Základní princip integrace systémů spočívá ve sběru dat jednotlivými systémy a následnému přenosu bezpečnostních protokolů a událostí do centralizované jednotky, kterou může být právě DLP nebo SIEM.

Nejčastějším způsobem komunikace mezi bezpečnostními programy a centrální platformou je **Syslog**. (Uetz 2024). Syslog (system logging protocol) je standardní protokol pro logování systémových zpráv v síťových zařízeních a v architektuře SIEM systémů hraje zásadní roli při zajišťování základního sběru dat z rozmanitých zdrojů. Při nastavování systému pro práci se Syslogem se definují dva hlavní parametry: facility (funkce), která udává, z jaké části systému nebo programu zpráva pochází, a severity (úroveň), která vyjadřuje závažnost dané události. (Ali 2025) Při integraci se na straně síťového zařízení typicky pouze nastaví IP adresa a port „syslog serveru“, což je ve skutečnosti adresa centralizované bezpečnostní platformy nebo nějakého log collectoru před ním. Využívané porty k přenosu zprávy jsou obvykle UDP 514 nebo TCP 601, ale oboje lze konfigurovat.

V rámci Syslogu je definována základní struktura: na začátku jsou v hlavičce metadata (čas, hostname, facility, severity) a za nimi samotná zpráva (payload). U starších zařízení je payload ve formě prostého textového řetězce, novější bezpečnostní systémy zprávu strukturují, typicky do formátu CEF, LEEF nebo JSON. Na straně SIEM běží Syslog daemon nebo vlastní listener, který tyto zprávy přijímá. Zároveň je v rámci SIEM nutné nastavit odpovídající datové vstupy nebo konektory pro příjem dat z konfigurovaných bezpečnostních platforem. (Tencent Cloud 2025)

Protože čistě textový Syslog je pro bezpečnostní systémy jako SIEM nebo DLP příliš komplikovaný na parsování, vznikly **standardizované formáty událostí**. Nejznámější z nich jsou CEF (Common Event Format), LEEF (Log Event Extended Format) a JSON

(JavaScript Object Notation). V praxi to vypadá tak, že payload syslog zprávy má jasně danou strukturu: nejprve hlavičku s informací o produktu, verzi a typu eventu, a za ní soubor klíčů a jejich hodnot.

Ukázka syntaxe formátu CEF:

```
Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

Ukázka syntaxe formátu LEEF:

```
Version|Vendor|Product|Version|EventID|<Tab>key1=value1<Tab>key2=value2
```

Ukázka syntaxe formátu JSON:

```
{
    "vendor": "Symantec",
    "product": "DLP",
    "version": "15.8",
    "event_id": 1001,
    "event_name": "File upload blocked",
    "severity": "Medium",
    "source_ip": "192.168.1.10",
    "destination_ip": "52.17.33.20",
    "user": "jnovak",
    "file_name": "data.pdf",
    "file_size": 204800,
    "action": "blocked"
}
```

Výhodou strukturovaného formátu je, že při správné konfiguraci centralizovaný systém dokáže napárovat názvy klíčů se svými interními poli. Hodně výrobců bezpečnostních produktů dnes nabízí možnost posílat logy v CEF nebo LEEF, typicky opět přes Syslog. Podobně to funguje s formátem JSON, který podporuje vnoření objektů. Některé systémy už generují události rovnou jako JSON objekt, ať už zabalený v Syslog zprávě, nebo poslaný přes HTTP API.

V případech, kdy nelze použít Syslog (například u Windows Event logů), se využívají **agenty**. V tomto kontextu jsou agenty malé softwarové balíčky instalované na server nebo koncová zařízení, které sledují lokální zdroje logů (Event Log, aplikační logy v souborech, databáze apod.) a posílají je na bezpečnostní platformu vlastním šifrovaným protokolem. Například u Windows systémů je často k dispozici speciální softwarový agent, který zajišťuje bezpečné doručení logů do SIEM nebo DLP kolektoru, často pomocí šifrovaného transportního mechanismu (např. VPN tunelu) (Podzins a Romanovs 2019)

Výhody agentů:

- Agenty mohou provádět lokální filtrování dat na základě předem stanovených kritérií, čímž se zajišťuje, že do centralizovaného systému jsou odesílány pouze relevantní bezpečnostní události. Tím se minimalizuje množství přenášeného "šumu" a snižuje zátěž na síťovou propustnost.

- Některé agenty mají schopnost provádět datovou normalizaci nebo kompresi ještě před odesláním, což opět snižuje zátěž samotného centrálního systému.

Nevýhody agentů:

- Instalace agentů může být časově náročná a velmi komplexní, pokud je třeba agenty instalovat na všechna pracovní koncová zařízení v podniku.
- Agenty mohou zpomalovat koncové zařízení, na kterém jsou instalovány. (Info-Tech Research Group 2025)

Ve Windows systémech často agenty čtou logy přes nativní API, případně ze specifikovaných logů jednotlivých aplikací, a ukládá si jejich stav (offset), aby po restartu nedošlo ke ztrátě dat. (Elastic 2025)

Tyto agenty často zajišťují i buffering, tedy pokud je centralizovaná platforma dočasně nedostupná, agenty ukládají logy lokálně a po obnovení spojení je odešlou označené časovým razítkem. (Hunters 2025) Pro Linux zařízení je typické, že část dat se posílá přímo jako Syslog, ale pro speciální aplikace nebo databáze se opět použije agent, který čte textové logy nebo databázové tabulky a převádí je do jednotného formátu. Ve výsledku to znamená, že přestože data pochází z vícero různých zdrojů, z pohledu centrálního systému všechna data přichází skrze jeden nebo pouze několik konektorů.

U moderních cloudových bezpečnostních produktů je Syslog často až druhořadý a hlavním integračním rozhraním je **REST API**. Zde se používají způsoby integrace logů, buď je v REST API nastaven endpoint, na který centrální platforma posílá dotazy (PULL sběr dat), nebo se využívají tzv. webhooks, což jsou uživatelsky definované zpětné volání směrem od REST API přes HTTPS do centralizovaného systému. (Atlassian 2025)

### 3.4.2 Problémy spojené s integrací bezpečnostních systémů

- **Data Overload:**
  Centrální platformy shromažďují logy z obrovského množství zdrojů, což může u velkých společností vést ke generování miliónů i miliard záznamů denně. (Bhatt et al. 2014). Většina těchto záznamů je tvořena pouhým "šumem" a false positive záchyty, které zbytečně zahlcují centrální systém i bezpečnostní týmy podniků a znemožňují včasné řešení skutečných incidentů. Tento jev je známý také jako "alert fatigue". (SearchInform 2025).

- **Neefektivní analýza logů:**
  Jak již bylo popsáno v předchozích kapitolách, logy analyzované centrální konzolí do ní přicházejí ve specifických formátech a je nejprve třeba je normalizovat do zpracovatelného stavu. Neúspěšná normalizace nebo nekonzistentní formáty mohou vést ke ztrátě detailů nebo celé zachycené události. "Neexistují logové soubory, které by SIEM systémy nedokázaly

analyzovat, podstatné je pouze to, jak efektivní daná analýza zdroje logů bude." (Podzins a Romanovs 2019)

- **Komplexita nasazení a provozu:**
  SIEM řešení není technologie "plug-and-play" (Info-Tech Research Group 2025) a to samé platí i pro systémy DLP. K jejich správnému fungování je potřeba, aby byly neustále optimalizovány týmem specialistů, čímž se zvyšuje účinnost zavedených pravidel a naopak snižuje množství false positive záchytů.

- **Vysoké náklady na vlastnictví, údržbu a personál:**
  Do celkových nákladů za systémy SIEM nebo DLP patří počáteční nákup softwaru, roční náklady na údržbu a licenční poplatky, které jsou často založené na objemu zpracovávaných logů. Typická platforma pro správu může stát 80 000 USD a archivní databáze 20 000 USD. Provoz operačního centra s nepřetržitým monitorováním a alespoň 20 specialisty může ročně vyjít na více jak 5 milionů USD. (Bhatt et al. 2014)

- **Složitost nastavení korelačních pravidel a bezpečnostních politik:**
  Úspěch detekce události závisí na síle korelačních pravidel v SIEM a aktuálnosti politik v DLP. Současná korelační pravidla v SIEM systémech jsou často považována za slabá, protože se spoléhají na základní booleovské řetězení událostí a kontrolu specifických cest útoku, které nemusí zachytit sofistikované hrozby. (González-Granadillo et al. 2021) Zároveň je komplikované nastavit korelační pravidla i bezpečnostní politiky tak, aby měly co nejmenší dopad na produktivitu zaměstnanců. V rámci průzkumu téměř 30 % respondentů uvedlo, že DLP politiky ztěžují zaměstnancům jejich práci. (De Sousa a Shahzad 2021)

### 3.4.3 Příklady výzkumů integrace bezpečnostních systémů

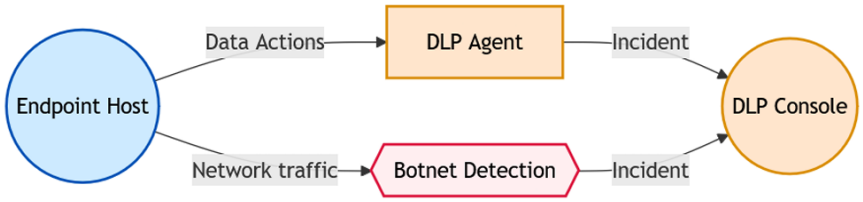
**Integrace DLP a algoritmů pro detekci botnetů**

Botnety jsou identifikovány jako jedna z hlavních příčin úniků dat a nesou zodpovědnost za přibližně 25 % všech incidentů v podnikovém prostředí. (Verizon 2022) Proto se jeden z výzkumů zaměřil na vývoj integrované architektury kombinující systémy Botnet Detection, které monitorují sítě, a systémy DLP, kontrolující pohyb dat. Korelováním informací z obou zdrojů lze identifikovat i jinak nenápadné varovné signály, že někde v síti dochází k exfiltraci dat. (Huralnyk et al. 2025)

Navrhovaná architektura systému zahrnuje čtyři komponenty, které lze vidět na obrázku 4:

1. Endpoint host (koncové zařízení)
2. DLP agent

3. Botnet detekční modul
4. DLP konzole




*Obrázek 4 - Integrovaná architektura Botnet Detection a DLP*
*Zdroj: (Huralnyk et al. 2025)*

DLP Agenty nainstalované v koncových zařízení detekují porušení nastavené bezpečnostní politiky, odešlou log do DLP konzole a zároveň vytvoří datový přenos, který projde Botnet Detection. Pokud algoritmus detekce botnetu zjistí podezřelé chování a DLP Agent současně detekuje, že dochází k pokusu odeslat soubory označené jako důvěrné, DLP konzole může přenos zablokovat.

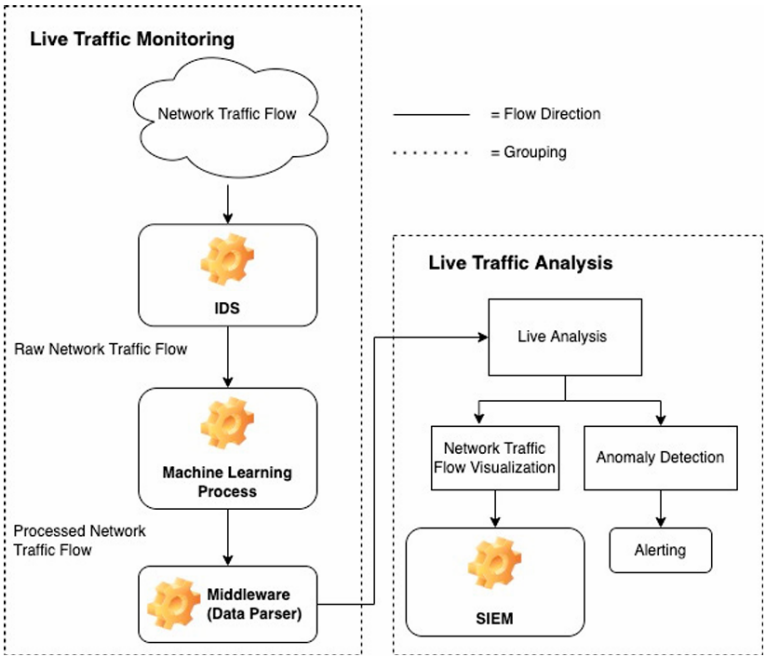
Pro ověření účinnosti byla provedena simulace útoku botnetu se zaměřením na únik kritických dat. Scénáře zahrnovaly pokusy o odeslání souborů prostřednictvím metod, které botnety často využívají: HTTP/HTTPS nebo DNS tunneling.

Experimentální výsledky ukazovaly vysokou účinnost integrovaného systému. Průměrná míra detekce u testovacích scénářů, včetně těch velmi komplexních, přesáhla 90 %. Průměrná doba odezvy se pohybovala v rozmezí 10 a 25 sekund a míra falešných poplachů nepřesáhla 3,5 %, což je v souladu s přijatelnými standardy.

**Integrace SIEM a IDS**

Jedna z oblastí výzkumu se zaměřila na integraci systému SIEM s IDS řešením s využitím techniky detekce anomálií. Účelem bylo vytvoření robustního a nízkonákladového systému, který by v reálném čase zpracovával síťový provoz pomocí strojového učení, detekoval anomální pakety a zobrazoval je v monitorovacím systému (SIEM). (Muhammad et al. 2023)

Architektura navrhovaného systému je vidět na obrázku 5.




*Obrázek 10 - Integrace systémů SIEM a IDS*
*Zdroj: (Muhammad et al. 2023)*

S ohledem na požadavek na rychlé a snadné nasazení byly pro implementaci systému vybrány open-source komponenty. Jako IDS řešení byl vybrán Zeek IDS, který je schopen provádět vícevrstvou analýzu síťových aktivit, doplněný o nástroj Slips, používaný pro analýzu strojovým učením v reálném čase. Pro monitorování a vizualizaci byl využit ELK Stack, což je kombinovaný komponent složený z nástrojů Elasticsearch, Logstash a Kibana.

Systém byl testován pomocí simulace kybernetického útoku typu DoS a testování zahrnovalo monitorování spotřeby systémových zdrojů CPU a RAM pro jednotlivé komponenty. Navržený systém úspěšně detekoval útok DoS a v reálném čase vizualizoval alerty skrze SIEM. Největší spotřebu zdrojů zaznamenal Elastisearch, který slouží jako centrální databáze a monitorovací jádro SIEM.

## 3.5 Vývoj a trendy v oblasti SIEM a DLP

Klíčovým směrem vývoje kybernetické bezpečnosti je konvergence bezpečnostních systémů s technologiemi AI a strojového učení. SIEM a DLP systémy prošly v rámci svého vývoje velkými změnami. Posunuly se od jednoduché korelace událostí nebo detekce na základě signatur k implementaci strojového učení i hlubokého učení (Pulyala 2024) a v dnešní moderní době se staly komplexními systémy poháněnými AI. Mezi jejich zásadní výhody patří:

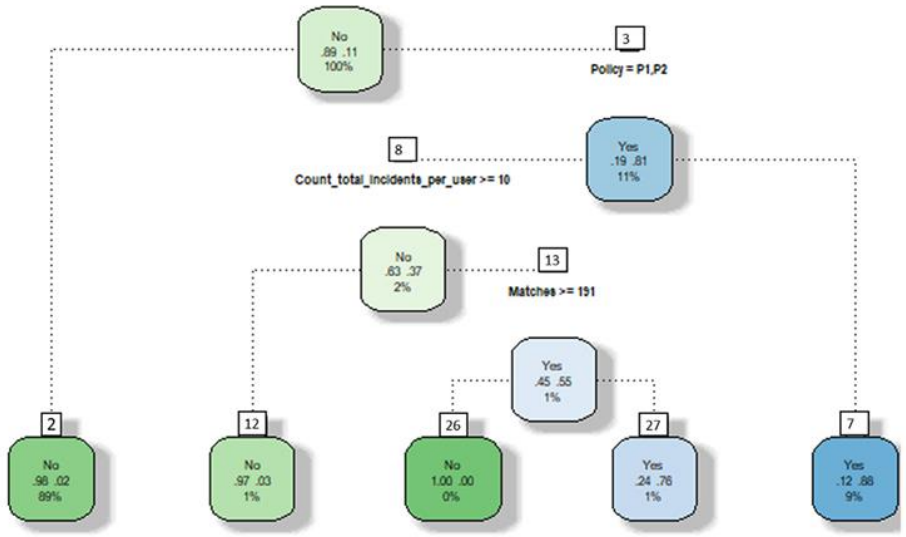
- Prediktivní (proaktivní) analýza
- Rychlejší detekce a automatizované reakce

- Nižší míra false positive záchytů
- Menší zátěž operačního centra
- Využití Analýzy chování uživatelů a entit (UEBA)
- Kontinuální rozvoj

Základem pro moderní systémy SIEM i DLP je strojové učení, které umožňuje analyzovat velké množství dat a hledat v nich vzorce, které jsou pro lidské oko neviditelné. (Ghelani 2023) Díky analýze historických dat mohou bezpečnostní systémy sloužit nejen k reakci na incidenty, ale být i proaktivní a detekovat potencionální budoucí útoky. Tvorba referenčních modelů zase posiluje identifikaci interních hrozeb pomocí odlišování běžného a neobvyklého chování uživatelů a systémů.

**Algoritmy strojového učení**

V oblasti DLP systému mohou být využity pokročilé analytické algoritmy strojového učení jako Decision Tree a Random Forest. Tyto algoritmy se zaměřují na analýzu historických dat incidentů a jsou schopny řešit komplexní klasifikační úlohy v reálném čase a proaktivně predikovat hrozby. (Faiz et al. 2019) To umožňuje oddělit a upřednostnit skutečné hrozby od nedůležitého šumu a zvyšuje efektivitu bezpečnostních týmů.




*Obrázek 6 - Vzorový strom pro experimenty založené na rozhodovacím stromu*
*Zdroj: (Faiz et al. 2019)*

Algoritmus Decision Tree je realizovaný pomocí dalšího algoritmu Classification and Regression Tree (CART) a slouží jako klasifikační nástroj, v rámci kterého dochází k přiřazování pravděpodobnosti rizik k analyzovaným incidentům. Random Forest je ensemble algoritmus, což znamená, že jeho podstatou je generování velkého počtu jednotlivých rozhodovacích stromů, na jejichž základě pak probíhá predikce. Předpokládá se, že predikce vytvořená souborem modelů je spolehlivější a přesnější než predikce jediného stromu.

Pomocí experimentální analýzy bylo prokázáno, že optimalizovaný model Random Forest dosahuje skvělých výsledků (až 95 % přesnost) v predikci úniků dat v e-mailových DLP systémech. (Faiz et al. 2019)

**Adaptive Misuse Detection**

Na základě nedávné studie bylo zjištěno, že minimálně 44 % běžně využívaných SIEM pravidel lze jednoduše obejít. (Uetz et al. 2023). Proto byla navržena nová metoda s názvem adaptivní detekce zneužití (Adaptive Misuse Detection), která k analýze logů využívá nejen běžná pravidla, ale zároveň pomocí strojového učení data srovnává se známými neškodnými událostmi. Navíc je pomocí metody možné detekovat, která pravidla se koncový uživatel pokusil obejít.

Základem adaptivní detekce je strojové učení, které se využívá k posouzení, zda se zachycená událost podobá normálnímu chování nebo naopak známému vzorci útoku. Datové sady s ukázkami útoků se nemusí vytvářet ručně, protože lze v modelu využít veřejně dostupné a pravidelně aktualizované databáze pravidel, které jsou často spravované řízenými komunitami na internetu.

Model je zároveň trénován na historických benigních událostech, tj. událostech, které nejsou hrozbou a v rámci podniku jsou považovány za obvyklou aktivitu. Tím se systém adaptuje na specifika cílového prostředí a jsou eliminována tzv. detekční slepá místa.

# 4 Vlastní práce

Data použitá v praktické části této studie byla poskytnuta vybraným podnikem a jeho zaměstnanci se svolením manažerů ochrany společnosti. Protože se tato data týkají především bezpečnostních složek podniku, jsou některé informace, včetně jména firmy, upraveny nebo zakryty. Úpravy dat nemají vliv na výsledky studie, pouze zaručují zachování bezpečnosti a integrity zkoumaného podniku.

## 4.1 Představení podniku

Zkoumaný podnik je dle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), kapitálová akciová společnost podnikající v energetickém sektoru. Svými parametry se řadí mezi velké podniky a je nadnárodní korporací působící v ČR i dalších státech Evropy. Společnost disponuje několika tisíci zaměstnanci a v ČR působí již několik desítek let.

Společnost si je plně vědoma bezpečnostních rizik v oblasti informačních a komunikačních technologií (ICT) a investuje do efektivního systému řízení s cílem zajistit úroveň informační a kybernetické bezpečnosti (IKB) v souladu s platnou legislativou a mezinárodními standardy. Informační aktiva podniku jsou zabezpečena z hlediska jejich důvěrnosti, dostupnosti a integrity. Řízení IKB ve společnosti zahrnuje mimo jiné oblasti:

- Politiky bezpečnosti informací (Information security policies)
- Organizace bezpečnosti informací (Organization of information security)
- Řízení přístupu (Access control)
- Fyzická ochrana a bezpečnost prostředí (Physical and environmental security)
- Bezpečnost komunikací (Communications security)
- Akvizice, vývoj a údržba systémů (System acquisition, development and maintenance)
- Zvládání incidentů bezpečnosti informací (Information security incident management)
- Soulad s požadavky (Compliance)

Bezpečnostních cílů se dosahuje skrze organizační, technické, procesní a personální opatření, které jsou adekvátně zaváděny v souladu s relevantními standardy, normami a legislativními požadavky, mezi které patří například:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

## 4.2 Zkoumané podnikové systémy

### 4.2.1 Podnikové operační centrum SOC

Ve zkoumaném podniku se kromě běžných citlivých dat, jako například data zákazníků, pohybují i další kriticky důležitá data, která vychází z povahy vykonávané činnosti. Vzhledem k citlivosti i rozsahu zpracování je napříč podnikovou infrastrukturou využíváno mnoho bezpečnostních systémů, od standardní antivirové ochrany až po pokročilé SIEM a ADRS řešení. Pro zefektivnění souvisejících procesů bylo v roce 201X do firmy integrováno bezpečnostní operační centrum SOC.

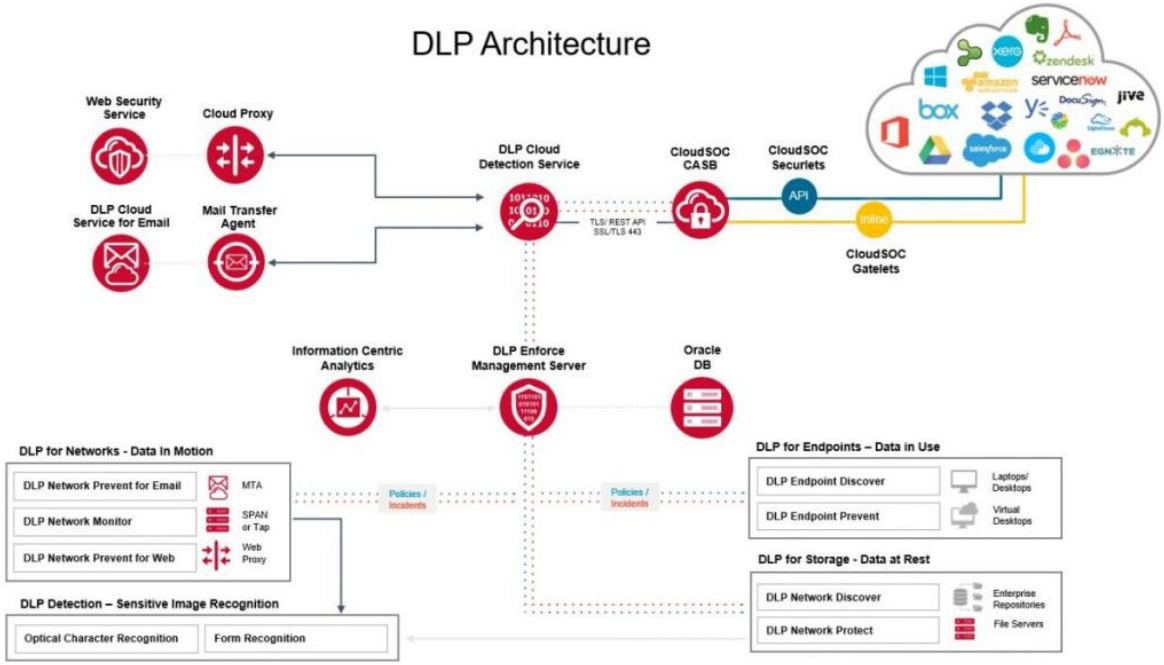
Jak bylo zmíněno v teoretické části práce, S. K. Bhatt ve své studii The Operational Role of Security Information and Event Management vyzdvihuje potřebu hierarchického uspořádání SOC, které kopíruje úrovně systému SIEM. Obdobný koncept je zavedený i ve zkoumaném podniku, kde jsou role členěny na:

- **Operátory SOC**, jejichž hlavní náplní práce je odbavování alertů v ESM (SIEM) konzoli a s tím související řešení požadavků a bezpečnostních událostí či incidentů. Dále se starají o nastavování výjimek. Potřeba výjimek ve využívaných bezpečnostních politikách je u velkých sítí jako je zkoumaný podnik běžnou záležitostí, ale je nutné při jejich nastavování postupovat obezřetně, aby se skrze ně neotevřelo zranitelné místo. Operátoři také provádějí kontrolu Dashboardů, tedy nastavených pohledů na data v SIEM, aktivně prohledávají logy a tvoří přednastavené reporty dle potřeby.
- **Specialisty SOC**, kteří primárně zajišťují provoz a funkci dohledových systémů. Tím je především myšleno zajištění kontinuálního logování napojených systémů a správa životního cyklu dat v souvislosti s retenčními lhůtami. Dále do jejich agendy spadá správa, aktualizace a revize dokumentace k napojeným systémům. To je podstatné hlavně kvůli regulačním normám a legislativním požadavkům. Mimo to se věnují i přípravě a koordinaci činností souvisejících s upgrady, odstávkami a hardeningem systémů nebo dohledu nad kapacitami datových skladů.
- **Analytiky SOC**, kteří zaprvé spolupracují na tvorbě definovaných postupů řešení bezpečnostních událostí či incidentů pro operátory SOC a zadruhé proaktivně vyhledávají, vyhodnocují a prověřují anomálie a podezřelé aktivity v nástrojích bezpečnostního dohledu. Tato činnost se nazývá Threat Hunting a analytici při ní kombinují data z logů a bezpečnostních nástrojů s hypotézami a znalostí technik útočníků, aby odhalili hrozby, které automatická detekce přehlédla. Na této úrovni také probíhá tvorba nových triggerů, alertů a reportů.

### 4.2.2 Stávající DLP řešení

Symantec DLP je navrženo jako distribuovaný systém, ve kterém se nachází tři oddělené, ale zároveň vzájemně provázané vrstvy: centrální správa (Enforce Server),

vrstva detekčních a preventivních uzlů (senzorů) a endpointový dohled nad koncovými zařízeními. Základní myšlenkou je, že organizace nejprve určí, co je považováno za citlivá data pomocí politik a klasifikačních pravidel a následně tyto politiky aplikuje napříč kanály, kde data nejčastěji odtékají, což mohou být např. webové služby, e-mail nebo síťové sdílení. Díky této modulární architektuře, jak je zobrazeno na obrázku 7, je možné škálovat výkon i organizační rozsah.




*Obrázek 7 - Architektura Symantec DLP*

*Zdroj: (Singh 2024)*

Jádrem systému je Enforce Server, který slouží jako centrální management platforma pro celý životní cyklus DLP dat. Skrze něj je poskytována webová administrační konzole, ve které se tvoří a spravují bezpečnostní politiky, konfiguruje se infrastruktura detekčních serverů a agentů a vyhodnocuje se porušení stanovených pravidel. Z hlediska architektury je důležité, že se zde neodehrává inspekce datových toků a samotná detekce. Ta probíhá na specializovaných uzlech blíže k datovým tokům.

Na Enforce Server je navázána Symantec databázová vrstva Oracle Database, která slouží jako centrální perzistentní uložiště pro veškerá systémová data a konfigurace. Jsou zde definována pravidla pro detekci citlivých dat, reakční pravidla (response rules) a nastavení jednotlivých detekčních serverů. Zároveň je zde každé zjištěné porušení bezpečnostní politiky zapsáno jako incident, včetně metadat o jeho vzniku a závažnosti. A pokud se využívají detekční profily, databáze zde uchovává definice těchto profilů pro technologie jako Exact Data Matching (EDM) nebo Indexed Document Matching (IDM).

Další samostatnou částí je Detection Server, tedy sada detekčních komponent pokrývajících celý životní cyklus informací v organizaci, které lze nasazovat modulárně podle scénářů ochrany dat v závislosti na jejich stavu, konkrétně Data at Rest, Data in Use a

Data in Motion, jak je popsáno v kapitole 3.2.1 v této práci. Typicky sem patří Network Monitor, který se umisťuje do síťové topologie tak, aby zachytával a analyzoval provoz opouštějící organizaci (např. Přes SPAN/TAP), Network Discover, který prochází síťová uložiště, Network Prevent a Network Protect zajišťující návazná opatření v případě záchytu. Dále se využívá Network Prevent for Email, který se integruje s poštovní infrastrukturou přes Mail Transfer Agent (MTA) a umožňuje kontrolu SMTP toku v reálném čase, a Network Prevent for Web napojený na webové proxy typicky pomocí ICAP, takže dokáže prohlížet HTTP/HTTPS/FTP obsah.

Poslední samostatnou vrstvou jsou endpointové agenty instalované na koncových zařízeních uživatelů v rámci organizace a k nim přidružené Endpoint servery sbírající data k incidentům. Endpoint Prevent se zaměřuje na monitorování a blokování úniku citlivých dat z koncového zařízení např. při kopírování na externí média nebo předáváním do aplikací v systému. Endpoint Discover naopak skenuje uložená data na koncových stanicích a hledá citlivý obsah at rest, případně umožňuje karanténu či automatizované zásahy.

Základem systému je jeho schopnost provádět analýzu obsahu a kontextu dat pomocí různých detekčních metod:

- **Exact Data Matching (EDM):** Technologie určená k detekci přesných dat ze strukturovaných zdrojů, jako jsou databáze zákazníků nebo zaměstnanců. Umožňuje například identifikovat kombinaci jména, příjmení a čísla účtu pocházejícího z jednoho konkrétního záznamu.
- **Exact Match Data Identifiers (EMDI):** Pokročilejší verze EDM, která je rychlejší a paměťově efektivnější. Na rozdíl od standardního EDM umožňuje provádět detekci lokálně přímo na endpoint agentovi bez nutnosti komunikace se serverem.
- **Indexed Document Matching (IDM):** Tato metoda využívá „otisků prstů“ (fingerprinting) k detekci přesných souborů nebo jejich částí a derivátů, což je ideální pro ochranu dokumentů s důvěrným obsahem, jako jsou zdrojové kódy nebo finanční zprávy.
- **Vector Machine Learning (VML):** Metoda založená na statistické analýze, která se učí rozpoznávat citlivý obsah na základě poskytnutých příkladů (pozitivních a negativních trénovacích sad). Je efektivní pro detekci nestrukturovaných dat, která jsou podobná již známým chráněným dokumentům.
- **Structured Data Matching (SDM):** Nová metoda, která umožňuje automaticky detekovat osobní údaje nebo finanční informace v tabulkovém formátu vloženém do nestrukturovaných dokumentů (např. v PDF nebo Excel).
- **Form Recognition:** Technologie schopná identifikovat naskenované nebo digitální obrázky formulářů na základě porovnání s definovanou galerií prázdných formulářů

### 4.2.3 Případová studie: bezpečnostní politika k ochraně obchodního tajemství

Obchodní tajemství představuje kategorii podnikových informací, jejichž únik může mít přímé finanční dopady a zároveň vystavit organizaci právním rizikům. Z hlediska

legislativy je ochrana obchodního tajemství povinností. Aby mohla být informace považována za obchodní tajemství i v právním smyslu, musí naplňovat určité znaky, například musí být prokazatelně chráněna odpovídajícími opatřeními.

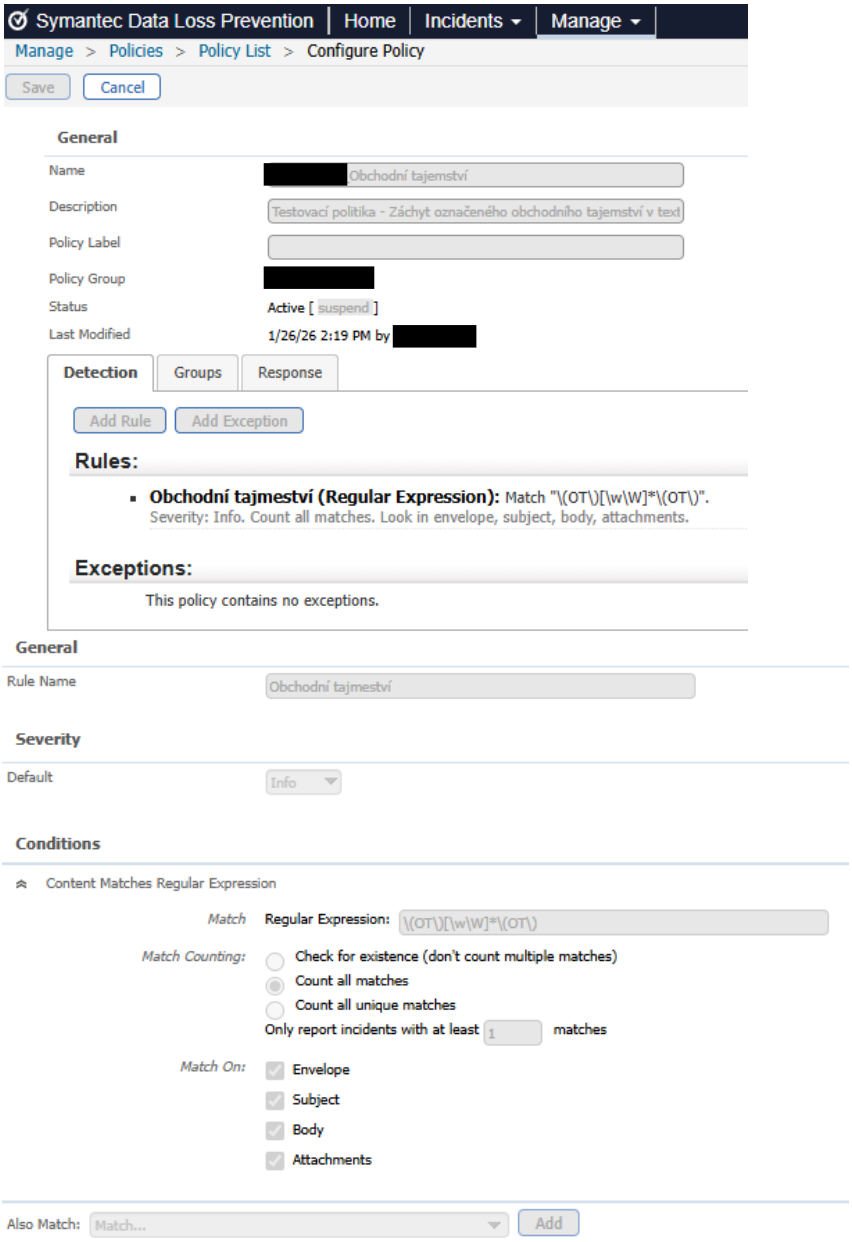
Zavedení konkrétních a systematických opatření, která by se cíleně zaměřovala na identifikaci a prevenci neoprávněné manipulace s informacemi spadajícími do obchodního tajemství, je ale v prostředí zkoumaného podniku problematické. Stávající nastavení bezpečnostních mechanismů řešilo ochranu citlivých informací spíše obecně a bez jasně definovaných pravidel pro tento typ obsahu.

Tato krátká případová studie se zaměřuje na vytvoření bezpečnostní politiky v prostředí DLP, jejímž účelem je posílit ochranu obchodního tajemství zejména v situacích, kdy dochází k manipulaci s těmito informacemi mimo bezpečnostní perimetr organizace. Za typické rizikové scénáře jsou považovány například pokusy o odeslání dokumentů nebo jejich částí do soukromých nešifrovaných e-mailových schránek, nahrávání na neautorizovaná cloudová úložiště, případně jiné formy sdílení mimo schválené komunikační kanály. Cílem politiky je takové jednání včas detekovat a iniciovat odpovídající reakci.

Významným omezením při tvorbě nové bezpečnostní politiky je nejednotné a nekonzistentní označování částí dokumentů jako obchodního tajemství napříč organizačními útvary. Interní předpisy uvádí, že dokumenty mají být označovány buď přímo v hlavičce souboru nebo ohraničením obchodního tajemství v textu zkratkami (OT) … (OT), ale z praktické zkušenosti vyplývá, že stejný typ informace může být v jednom týmu formálně označen a v jiném nikoli, případně je označení provedeno odlišnými způsoby.

V první fázi procesu byla gestorem zřizované politiky zadána nová žádost ve firemním požadavkovém systému. Požadavek prošel standardním schvalovacím workflow a zároveň proběhlo jeho posouzení auditory DLP, než byl předán metodikům DLP k vyřešení.

Dále bylo vytvořeno pravidlo pro záchyty ve formě regulárního výrazu „\(OT\)[\w\W]*\(OT\)“, kterým byly sledovány úseky textu ohraničené dvěma výskyty textového řetězce „(OT)“. Do politiky v tuto chvíli nebyly zavedeny žádné výjimky, jak je vidět na obrázku 8, ale na základě zkušeností z praxe to do budoucna nelze vyloučit.




*Obrázek 8 - Pravidla politiky pro ochranu obchodního tajemství*

*Zdroj: (Vlastní zpracování)*

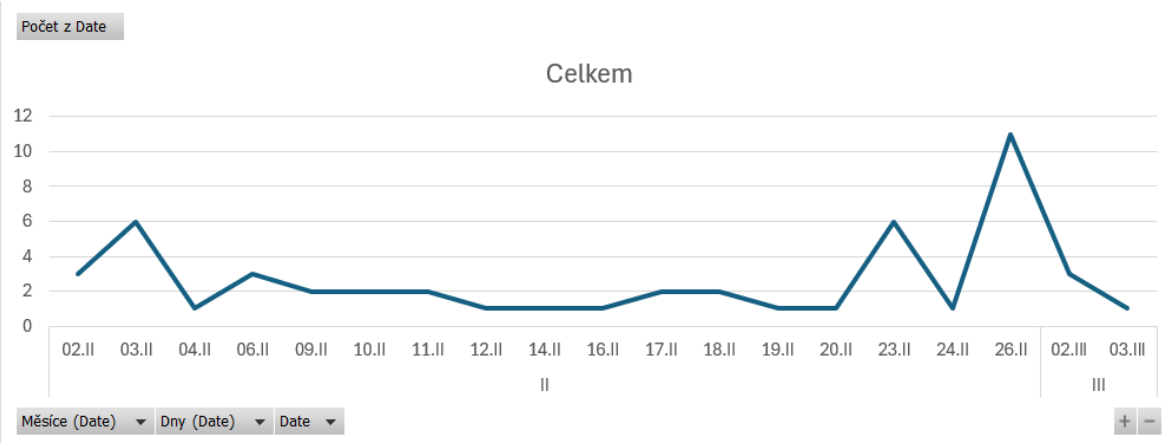
Volba Match Counting určuje, jak DLP počítá nalezené shody a kdy má vyvolat incident. Je možné zde nastavit, zda je pro nás důležité, kolikrát se shoda v kontrolovaných datech objeví, případně zda jde o unikátní výskyty. V tomto případě je politika nastavena na možnost počítání všech výskytů regexu bez ohledu na to, zda jsou jedinečné nebo ne. Minimální práh je dán už na jeden výskyt.

Match On je podstatné pro definici, v kterých částech zprávy se má regulární výraz hledat. Protože obchodní tajemství může mít mnoho forem, jsou zde pro jistotu označeny všechny možnosti a to:

- Envelope – SMTP obálka (příjemce, odesílatel atd.)

- Subject – předmět e-mailu
- Body – tělo zprávy
- Attachments – přílohy zprávy

V období od 02.02.2026 do 03.03.2026 bylo testovací bezpečnostní politikou zachyceno 50 eventů. Záchyty se objevovaly téměř denně s několika výkyvy, z nichž ten největší byl ke konci února (26.02., 11 záchytů), jak lze vidět v grafu 4. Nicméně, významnou část záchytů tvořily false positive (přesné číslo si garanti politiky nepřejí uvádět), jelikož se zkratka „OT“ běžně využívá pro označení operačních technologií a v mnoha případech se v textu objevuje více jak jednou, což vede ke spuštění regexového pravidla politiky.



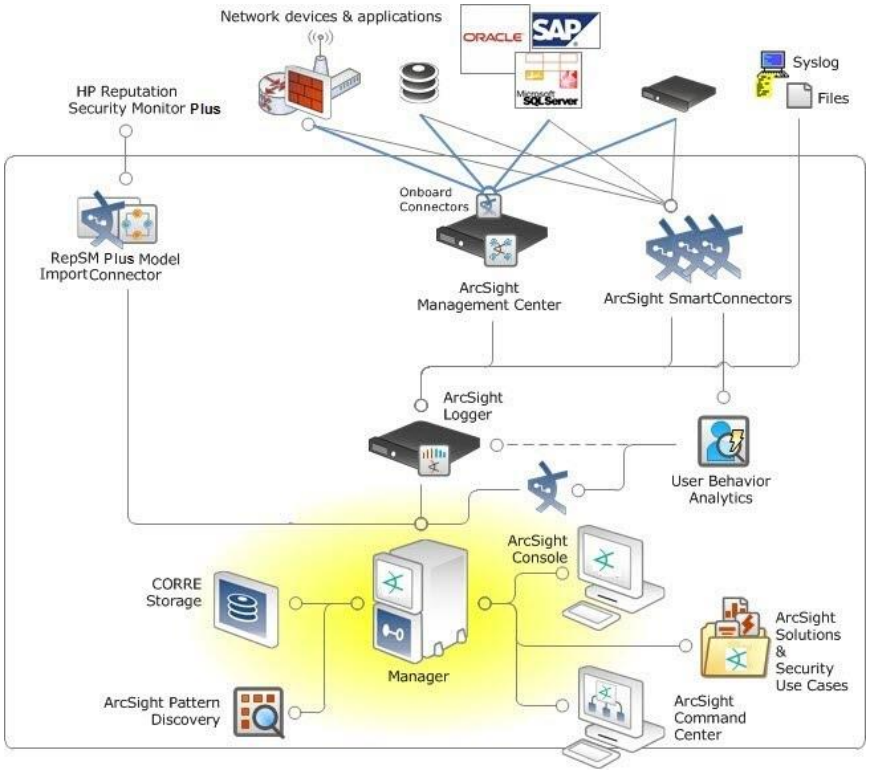

*Graf 4 - Vývoj záchytů pro bezpečnostní politiku OT*
*Zdroj: (Vlastní zpracování)*

Testování potvrdilo, že bez konzistentního a zároveň jednoznačného způsobu klasifikace je technické nastavování bezpečnostních opatření a vyhodnocování souvisejících záchytů obtížné. Velmi vysoký výskyt falešně pozitivních záchytů vede k nepřiměřené časové zátěži. V současné době se proto v podniku pracuje na změně způsobu označování obchodního tajemství napříč organizačními útvary tak, aby byla budoucí klasifikace sjednocená, nezaměnitelná a zároveň technicky využitelná pro nastavení účinných kontrolních mechanismů prostřednictvím DLP.

### 4.2.4 Stávající SIEM platforma

Systém ArcSight Enterprise Security Management (ESM) představuje softwarové řešení typu SIEM, které integruje tradiční monitorování bezpečnostních událostí s pokročilou síťovou inteligencí a kontextovou korelací. Základem fungování ESM je schopnost sbírat data z heterogenních síťových uzlů (firewally, IDS, operační systémy, databáze) prostřednictvím tzv. SmartConnectorů. Ty převádějí údaje o událostech ze zařízení do normalizovaného schématu Common Event Format (CEF), které se stává výchozím bodem pro korelaci. Normalizace zahrnuje také sjednocení časových pásem a převod priorit a závažností na společnou škálu ESM.

Správce zpracovává a ukládá data událostí v CORR-Engine, což je proprietární datové úložiště optimalizované pro vysokou rychlost zpracování událostí a efektivní prohledávání historických dat. Pracovníci SOC sledují události pomocí konzole ArcSight Console a ArcSight Command Center, která může spouštět zprávy, vyvíjet zdroje, provádět vyšetřování a správu systému. Mimo to ESM zahrnuje možnosti Pattern Discovery, tedy funkce pro odhalování neznámých hrozeb a útoků typu „zero-day“ bez nutnosti předem definovaných pravidel. Základní architektura ESM, kterou lze vidět na obrázku 9 se stává rámcem spravujícím tok událostí, usnadňující analýzu událostí a poskytující bezpečnostní výstrahy a reakce na incidenty.




*Obrázek 9 - Architektura ArcSight Enterprise Security Management*
*Zdroj: (Open Text Corporation 2025)*

ESM také automaticky přiřazuje každé události prioritu (0–10) na základě vzorce, který zohledňuje závažnost události, důvěryhodnost modelu aktiva, relevanci útoku vzhledem k otevřeným portům a kritičnost daného aktiva pro podnik

**SmartConnectors**

SmartConnectors představují z pohledu architektury SIEM inteligentní rozhraní mezi koncovými síťovými uzly a centrálním manažerem (ArcSight Manager). Jejich primárním účelem je transformovat nesourodá data z různých zařízení do jednotného, standardizovaného formátu, který je následně využit pro korelaci a analýzu. Tyto konektory jsou schopny sbírat data z více než 400 typů zařízení prostřednictvím různých technik, jako je čtení logů, SNMP trapy, syslog nebo přímé dotazy do databází. Normalizace zahrnuje

sjednocení struktury polí, formátu časových razítek (převod na UTC) a škálování závažnosti událostí (tzv. agent severity) na společnou stupnici ESM.

Podle způsobu získávání dat a charakteru zdroje se rozlišují různé typy konektorů:

- **Standardní SmartConnectors:** Předem konfigurované konektory pro konkrétní produkty a systémy běžně využívané v komerčním prostoru.
- **FlexConnectors:** Umožňují vytvořit vlastní SmartConnectors na míru zdroji, aby docházelo k normalizaci a parsování z nestandardních formátů.
- **Model Import Connectors:** Neslouží ke sběru událostí, ale k importu identit uživatelů a informací o aktivech z externích systémů (např. Active Directory) pro obohacení kontextu v ESM.
- **Scanner Connectors:** Přebírají výstupy z nástrojů pro skenování zranitelností a transformují je do ESM Asset Modelu.

Nad rámec prosté normalizace provádějí SmartConnectors tzv. kategorizaci, což je proces přiřazování srozumitelných charakteristik událostem na základě šesti kritérií:

- objekt (Object),
- chování (Behavior),
- výsledek (Outcome),
- technika (Technique),
- skupina zařízení (Device Group)
- a význam (Significance).

Tato kategorizace umožňuje analytikům a operátorům SOC psát pravidla a filtry nezávisle na konkrétním typu zařízení, protože pracují s lidsky čitelnými pojmy namísto kódů specifických pro poskytovatele systémů.

**Technická odolnost a bezpečnost**

SmartConnectors zajišťují integritu a dostupnost dat pomocí pokročilých funkcí jako je Caching, který v případě nedostupnosti centrálního manažera (např. při výpadku sítě) ukládají SmartConnectors události do komprimované diskové mezipaměti. Po obnovení spojení jsou data postupně odeslána k dalšímu zpracování. Další možností je Batching, kdy jsou události odesílány v dávkách (standardně po 100 událostech nebo každou sekundu). Podstatné je i šifrování. Komunikace mezi konektory a Manažerem probíhá standardně přes zabezpečený protokol HTTPS. Konektory navíc podporují šifrování citlivých polí události (Format Preserving Encryption) pro dodržení regulatorních požadavků.

### 4.2.5 Přenos dat v rámci podniku

Na obrázku 10 je zachycený model přenosu událostí ze systému Symantec DLP do prostředí ArcSight SIEM v rámci zkoumaného podniku. Tok začíná ve třech kategoriích zdrojů událostí již dříve popsaných v kapitole 3.2.1: Data in Motion, Data at Rest a Data in Use. Data in Motion sleduje především pohyb dat v podnikové síti, včetně webového

provozu, e-mailové komunikace apod. Tok směřuje do modulů Network Monitor, který plní roli detekce, a Network Prevent, skrze který se realizuje výkonná vrstva pravidel pro preventivní zásahy. U kategorie Data at Rest vstupují data do modulu Discovery, kde se provádí skenování uložených dat ve firemních databázích. Data in Use jsou zajištěna pomocí enpointových agentů instalovaných na většině pracovních zařízeních v rámci podniku.

Dalším krokem je centralizace těchto dílčích výstupů ve vrstvě agregace událostí v Detection Server DLP řešení a následně přenos do konzole, která má roli administrační vrstvy. Enforce Server přebírá výsledky detekce a připravuje je pro další správu, včetně exportu do navazujících systémů.

Standardním formátem pro přenos dat do systému SIEM je ve firmě formát CEF. Komponenty Syslog export a Transport zajišťují převod dat do tohoto strukturovaného formátu a následně i jejich přenos prostřednictvím TCP (dříve byl ve firmě využíván i protokol UDP).

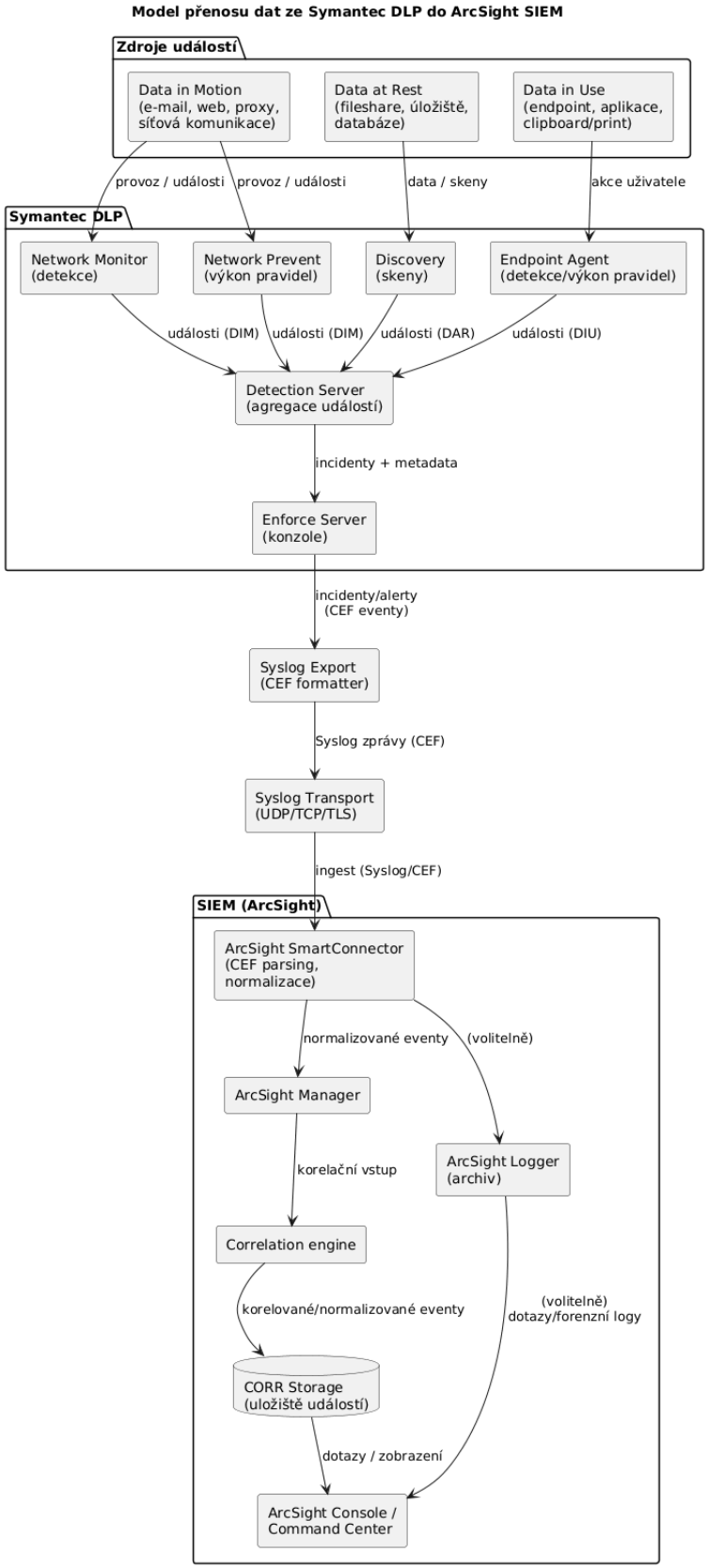
Data vstupující do prostředí SIEM jsou nejprve zpracovány v komponentě SmartConnector, která plní přednastavenou funkci parsování a normalizace přijímané CEF zprávy. Firma umožňuje i tvorbu nových FlexConnectors pro předem nedefinované formáty. (tuto činnost mají na starost analytici SOC), ale zde to není potřeba.

Jelikož nedochází k přenosu všech dat zachycených systémem DLP, byl pro bezpečnostní politiky definován následující formát obsahující pouze přenášené atributy:

*CEF:0|SYMANTEC|DLP|CEF V0.1|INCIDENT|$POLICY$|$SEVERITY$|*
*dvcpid=$INCIDENT_ID$ msg=$POLICY$ cn1=$MATCH_COUNT$*
*cn1Label=MatchCount cs1=$SENDER$ cs1Label=Sender cs2Label=Recipient*
*cs3=$OCCURRED_ON$ cs3Label=TimeStamp cs4=$SUBJECT$ cs4Label=EmailSubject*
*filePath=$ATTACHMENT_FILENAME$ shost=$ENDPOINT_MACHINE$*
*suser="$ENDPOINT_USERNAME$" act=$STATUS$ cs2=$RECIPIENTS$*

Ze SmartConnector vychází hlavní a vedlejší proud. Hlavní tok pokračuje jako normalizovaný event do ArcSight Manager, který zde funguje jako centrální aplikační vrstva a předává data dále do korelačního enginu. Ten nad přijatými událostmi vyhodnocuje vztahy a významné souvislosti z hlediska bezpečnosti. Výstupem jsou korelované a normalizované eventy, které jsou ukládány do CORR Storage, tedy úložiště událostí. Koncovým bodem hlavního toku a prezentační vrstvou je ArcSight konzole, resp. Command Center. Zde analytici SOC vidí finální zobrazení a filtrované dotazy.

Vedle hlavního toku existuje i volitelná archivní větev. Ze SmartConnector mohou normalizované eventy směřovat také do ArcSight Logger, který slouží jako archiv. Z Loggeru pak mohou do konzole směřovat volitelné dotazy a forenzní logy.




*Obrázek 10 - Komponentový UML diagram přenosu dat z DLP do SIEM*

*Zdroj: (Vlastní zpracování pomocí PlantUML)*

## 4.3 Cíle testování

Cílem testování je ověřit spolehlivost, rychlost a kvalitu zpracování bezpečnostních událostí při přenosu ze systému Symantec DLP do systému ArcSight SIEM. Konkrétně se ověřuje, zda:

- dojde ke spolehlivému předání a zpracování všech sledovaných bezpečnostních událostí bez vzniku ztrát nebo duplicit;
- po obnově přenosu je v co nejkratším čase zpracována fronta požadavků v backlogu DLP, aby se zpracování vrátilo do režimu blízkému real-time;
- dochází ke korektnímu parsování dat a mapování klíčových atribut do očekávaných polí.

Testování je rozděleno do dvou vzájemně se doplňujících scénářů. První scénář ověřuje kvalitu dat při standardním provozu a sleduje, zda vestavěné parsery v SIEM korektně zpracují specifické hraniční případy ve struktuře CEF. Druhý scénář je navržen jako zátěžový chaos test, při němž je dočasně přerušen datový tok mezi DLP a SIEM, aby bylo možné vyhodnotit odolnost integrace vůči krátkodobému výpadku.

Výsledky testů následně slouží jako podklad pro vyhodnocení, zda stávající integrace splňuje požadavky podniku na úplnost a konzistenci bezpečnostních událostí pro účely monitoringu a incident response

| Test scénář | Název | Počet test politik | Počet test eventů |
|---|---|---|---|
| **TC-01** | Validace parsování a kvality dat | 7 | 7 |
| **TC-02** | Chaos test: výpadek toku z DLP do SIEM | 10 | 100 |

*Tabulka 5 - Testovací scénáře*
*Zdroj: (Vlastní zpracování)*

### 4.3.1 Omezení při testování

Při realizaci testů jsou použité výhradně testovací politiky, popsány v následujících kapitolách, a neškodná testovací data, aby nedošlo k zásahu do reálných citlivých informací nebo k narušení běžného provozu podniku. Po celou dobu testování je současně sledován případný dopad na produkční prostředí.

Při plánování testování bylo nutné zohlednit také personální a provozní omezení na straně správců systémů DLP a SIEM i pracovníků bezpečnostního operačního centra SOC. Tito zaměstnanci zajišťují každodenní provoz klíčových bezpečnostních technologií a jejich práce je průběžně zatěžována neustálým přílivem nových záchytů, které vyžadují okamžitou pozornost. Z tohoto důvodu nebylo možné testování navrhnout jako rozsáhlý experiment s velkým objemem dat nebo s dlouhodobým zásahem na systémy. Pracuje se proto s omezeným, ale cíleně vybraným vzorkem testovacích dat, který umožňuje ověřit klíčové vlastnosti integrace bez nadměrného zatížení odpovědných pracovníků.

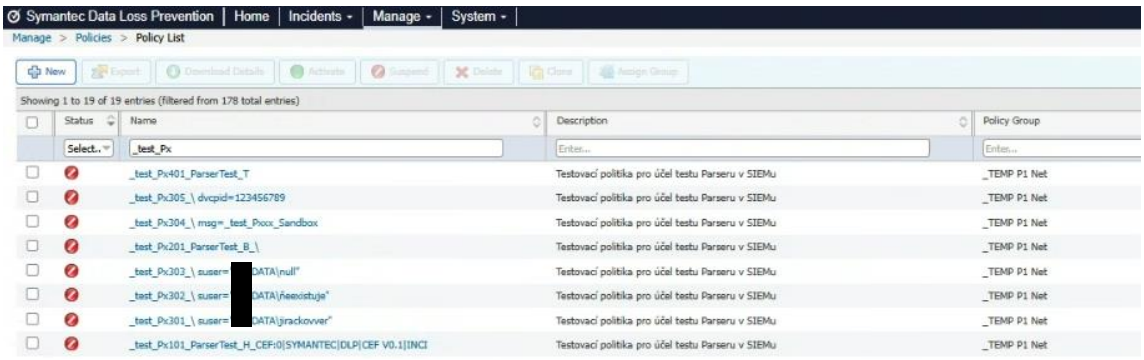
## 4.4 TC-01 Validace parsování a kvality dat

Cílem tohoto scénáře je ověřit správnost parsování a mapování polí z CEF při standardním přenosu, a to i v případech, kdy vstupy obsahují speciální znaky nebo pokusy o injekci kombinace klíč=hodnota. Výstupní data by měla být přesná, konzistentní a zároveň mít vypovídací hodnotu pro forenzní vyšetřování bezpečnostních událostí.

**Hypotéza pro TC-01**

Při standardním přenosu bude 100 % všech testovacích událostí z DLP doručeno do SIEM bez ztrát, neobjeví se žádné chyby při parsování a mapování klíčových atribut ani nedojde k zařazení událostí mezi neúplně zpracované záznamy.

### 4.4.1 Příprava testovacích politik




*Obrázek 11 - Seznam politik pro TC-01*
*Zdroj: (Vlastní zpracování)*

V souladu s omezeními testování byly použity pouze testovací bezpečnostní politiky vytvořené v Symantec DLP řešení. Celkem bylo pro účely testovacího scénáře připraveno 7 bezpečnostních politik, jejich souhrn je vidět na obrázku 11 a v tabulce 6.

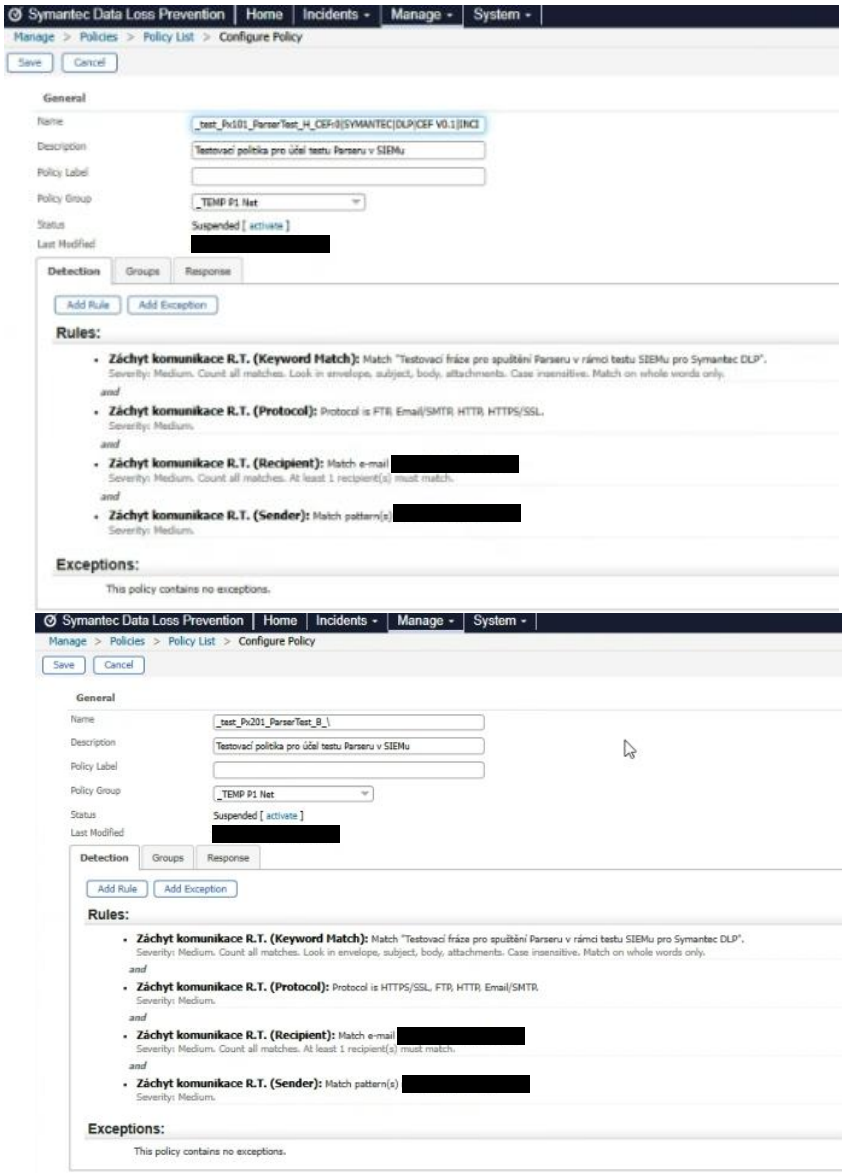
| Kategorie | Název politiky | Počet test eventů |
|---|---|---|
| A | _test_Px101_ParserTest_H_CEF:0\|SYMANTEC\|DLP\|CEF V0.1\|INCI | 1 |
| A | _test_Px201_ParserTest_B_\ | 1 |
| B | _test_Px301_\ suser="DATA\jirackovver" | 1 |
| B | _test_Px302_\ suser="DATA\ňeexistuje" | 1 |
| B | _test_Px303_\ suser="DATA\null" | 1 |
| C | _test_Px304_\ msg=_test_Pxxx_Sandbox | 1 |
| C | _test_Px305_\ dvcpid=123456789 | 1 |

*Tabulka 6 - Seznam politik pro TC-01*
*Zdroj: (Vlastní zpracování)*

**Kategorie A**

Do kategorie A byly zařazeny dvě politiky, které se zaměřily na speciální (řídicí) znaky. Speciální znaky mají zvláštní význam v programování nebo datových formátech. Patří sem například |, \, /, @, #, %, & nebo =. V kontextu zpracování dat mohou ovlivnit parsování nebo interpretaci obsahu, proto je nutné s nimi pracovat opatrně.

Při přípravě testovacích politik se vycházelo z manuálu *Implementing ArcSight Common Event Format (CEF) - Version 26* (Open Text, 2023), v kterém je doporučováno speciální znaky ecapovat, tedy umístit před ně tzv. únikový znak, v tomto případě zpětné lomítko, kterým se jim odebere speciální funkce. V dokumentu byl kladen důraz především na znaky v hlavičce CEF, zde se jedná o: *CEF:0|SYMANTEC|DLP|CEF V0.1|INCIDENT|$POLICY$|$SEVERITY$|*.




*Obrázek 12 - Testovací politiky Px101 a Px201*

*Zdroj: (Vlastní zpracování)*

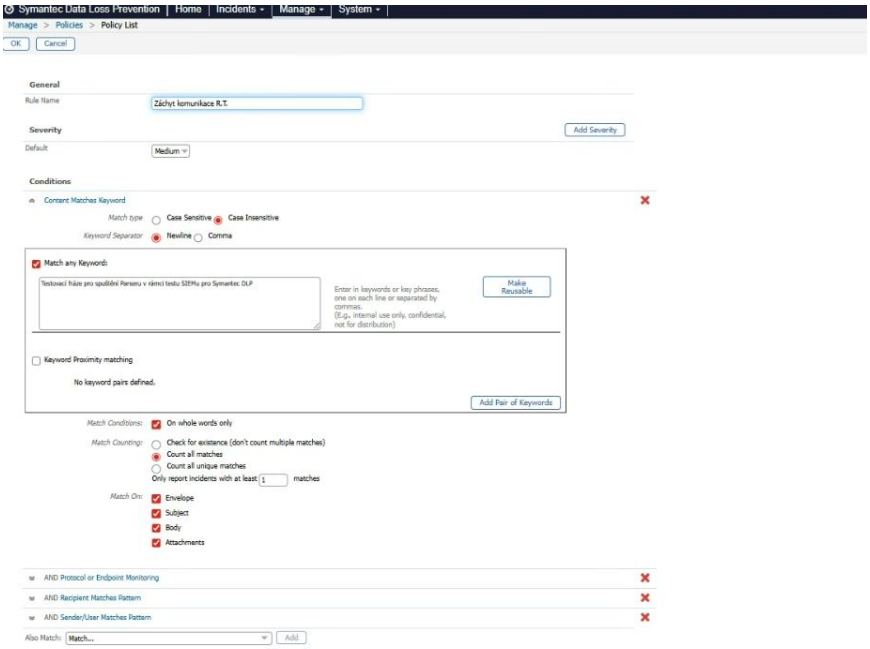
V obou politikách, zobrazených na obrázku 12, byly řídicí znaky vložené přímo do názvu politik, která se následně objevuje ve formátu CEF jak v hlavičce, tak v samotné zprávě.

- U politiky Px101 bylo do názvu přepsána část hlavičky CEF, důležité byly především znaky |, kterými se hlavička odděluje.
- V politice Px201 byl na konec názvu vložen znak \

Policy Group rozhoduje o tom, jaké skupině řešitelů přijde informace o vzniku bezpečnostní události. V tomto případě byla u všech politik nastavena dočasná testovací skupina, aby neměly záchyty dopad například na reporty se skutečnými záchyty.

V rámci obou bezpečnostních politik byly nastaveny následující pravidla pro vytvoření záchytu:

- Shoda s klíčovou frází:




*Obrázek 13 - Pravidla testovací politiky Px101*

*Zdroj: (Vlastní zpracování)*

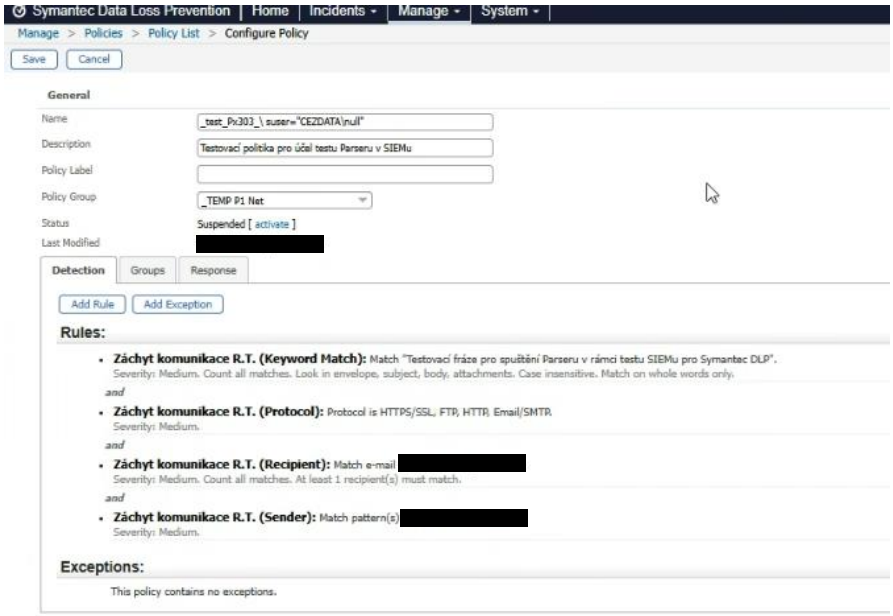
Jak je vidět na obrázku 13, Symantec DLP umožňuje nastavit jedno nebo více klíčových slov, případně klíčových frází, které se vyhledávají v různých částech zprávy. Zde byla zvolena specifická fráze unikátní pro testování: „Testovací fráze pro spuštění Parseru v rámci testu SIEMu pro Symantec DLP“. Hledala se alespoň jedna shoda celých slov v obálce, předmětu, těle i příloze zprávy.

- Shoda protokolů: Vyhledávání probíhalo na protokolech FTP, Email/SMTP, HTTP a HTTPS/SSL
- Shoda příjemce: Aby došlo ke spuštění politiky, příjemcem musela být specifická e-mailová adresa. Zvolena byla soukromá e-mailová schránka.

- Shoda odesílatele: Aby došlo ke spuštění politiky, odesílatelem musela být specifická e-mailová adresa. Zvolen byl pracovní e-mail.

K aktivaci politiky musí být splněna všechna výše popsaná pravidla (pravidla jsou spojena logickou spojkou AND).

### Kategorie B




*Obrázek 14 - Testovací politika Px303*

*Zdroj: (Vlastní zpracování)*

Kategorie B se zaměřila na injekci dvojice klíč=hodnota pro atribut *suser* s cílem zjistit, zda nedojde k přemapování již vyplněného atributu, viz obrázek 14. Injekce je obvykle situace, kdy je do aplikace nebo systému vložen škodlivý nebo neočekávaný vstup, který je následně chybně vyhodnocen jako příkaz či součást programu. K tomu obvykle dochází tehdy, když systém nedostatečně kontroluje uživatelská data a místo běžného textu je interpretuje jako vykonatelný obsah.

Atribut *suser* neboli source user je standardním atributem ArcSight CEF, jak je vidět na obrázku 15. Pro potřeby podniku se zde mapuje e-mailová adresa uživatele, který byl identifikován jako zdroj eventu. Jedná se tedy o velmi důležitý atribut z hlediska forenzního vyšetřování.

| | | | | | |
|---|---|---|---|---|---|
| 0.1 | suser | sourceUserName | String | 1023 | Identifies the source user by name. Email addresses are also mapped into the UserName fields. The sender is a candidate to put into this field. |

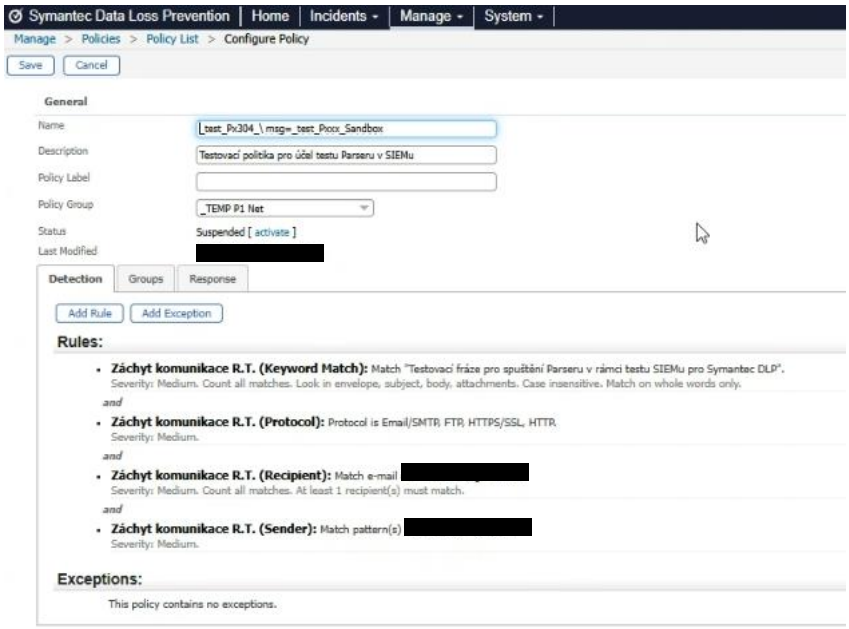
*Obrázek 15 - Atribut suser*

*Zdroj: (Open Text. 2023)*

Pravidla pro vytvoření záchytu byla stejná jako u Kategorie A a použity byly tyto hodnoty:

- suser = „DATA\null“
- suser=“DATA\ňeexistuje“
- suser=“DATA\jirackovver“

**Kategorie C**

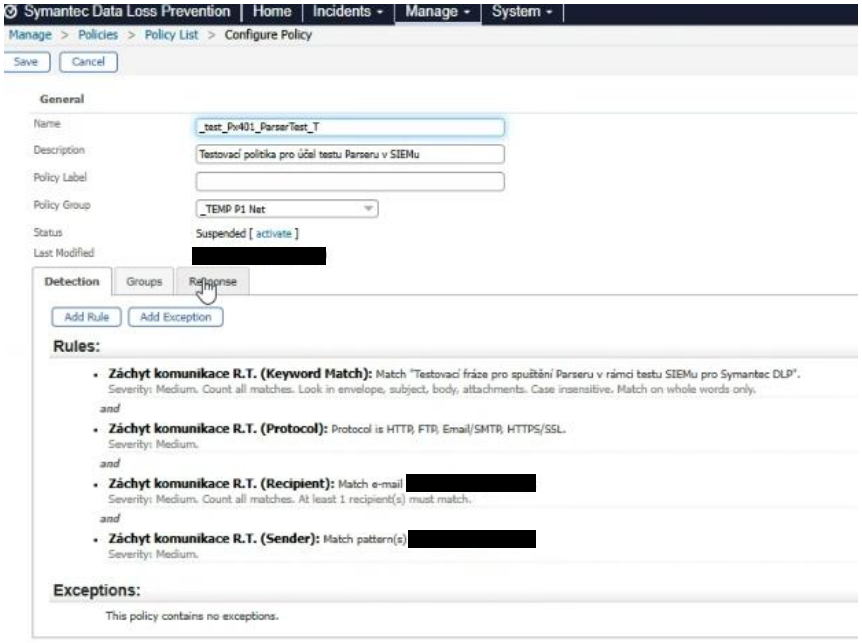



*Obrázek 13 - Testovací politika Px304*

*Zdroj: (Vlastní zpracování)*

Na obrázku 16 je zobrazena kategorie C, která se taktéž zaměřila na injekci klíč=hodnota, se stejnými pravidly záchytu, ale s odlišnými atributy. Konkrétně se jednalo o *msg* neboli message, který v tomto případě mapuje opět název politiky do těla zprávy místo hlavičky, a atribut dvcpid či device PID, tedy unikátní číslo zařízení, na kterém vznikl event. Hodnoty byly:

- msg=_test_Pxxx_Sandbox
- dvcpid=123456789




*Obrázek 14 - Testovací politika Px401*

*Zdroj: (Vlastní zpracování)*

### 4.4.2 Průběh testu

Před samotným spuštěním testů proběhla kontrola a nastavení testované prostředí tak, aby bylo možné jednoznačně sledovat celý tok událostí od jejich vzniku v systému Symantec DLP až po jejich zobrazení v prostředí ArcSight. Z hlediska integrační architektury bylo ověřeno, že události jsou exportovány ve formátu CEF, přenášeny prostřednictvím syslogu a dále zpracovávány komponentou SmartConnector. Proces testování byl sledován v následujícím softwaru:

- Symantec Data Loss Prevention (konzole DLP)
- ArcSight Console (konzole SIEM)
- Tcpdump

Před spuštěním tcpdump byla provedena kontrola, zda je na discích dostatek volného prostoru pro záchyt paketů, viz obrázek 18,

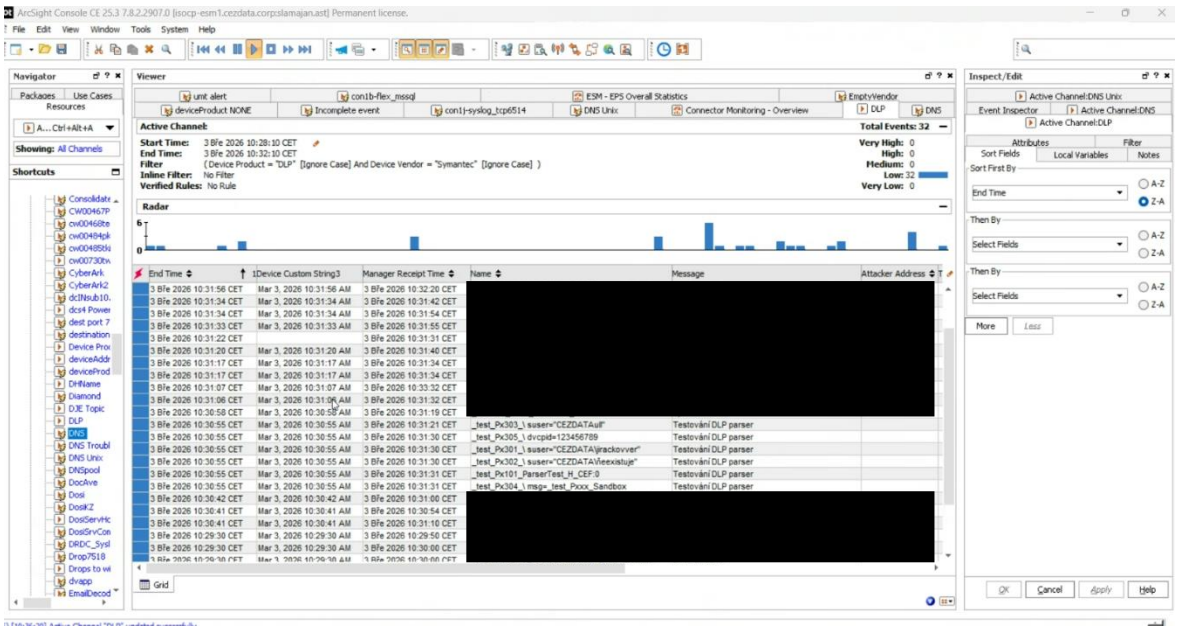
```
[PROD] [root@cl00219:~]#df -h
Filesystem                    Size  Used Avail Use% Mounted on
devtmpfs                       24G     0   24G   0% /dev
tmpfs                          24G  1.3M   24G   1% /dev/shm
tmpfs                          24G 1000K   24G   1% /run
tmpfs                          24G     0   24G   0% /sys/fs/cgroup
/dev/mapper/VolGroup00-lvroot  20G  9.6G   10G  50% /
/dev/mapper/VolGroup00-lvvar  9.8G  2.1G  7.7G  22% /var
/dev/mapper/VolGroup00-lvtmp   10G  105M  9.9G   2% /tmp
/dev/mapper/vgdata-lvdata      99G   28G   71G  29% /opt/arcsight
/dev/sda2                    1014M  480M  535M  48% /boot
/dev/sda1                     256M  5.8M  250M   3% /boot/efi
/dev/mapper/VolGroup00-lvhome  2.0G  456M  1.5G  23% /home
tmpfs                          4.7G     0  4.7G   0% /run/user/93739
tmpfs                          4.7G     0  4.7G   0% /run/user/74724
tmpfs                          4.7G     0  4.7G   0% /run/user/93432
[PROD] [root@cl00219:~]#pwd
/root
[PROD] [root@cl00219:~]#tcpdump -i any -A src host winpdlpes.   :data.corp
```

*Obrázek 15 - Kontrola tcpdump*

*Zdroj: (Vlastní zpracování)*

Jelikož měly všechny testovací bezpečnostní politiky nastaveny jednotná pravidla záchytu, proběhla jejich aktivace souběžně. Z jedné předdefinované e-mailové schránky do druhé byla odeslána zpráva s vepsanou klíčovou frází, čímž se zároveň splnily všechny čtyři podmínky.

V systému ArcSight, na obrázku 19, se nastavilo filtrování tak, aby byly zachytávány pouze eventy od produktů Symantec a pouze v omezeném časovém okně.



*Obrázek 19 - ArcSight Console TC-01*

*Zdroj: (Vlastní zpracování)*

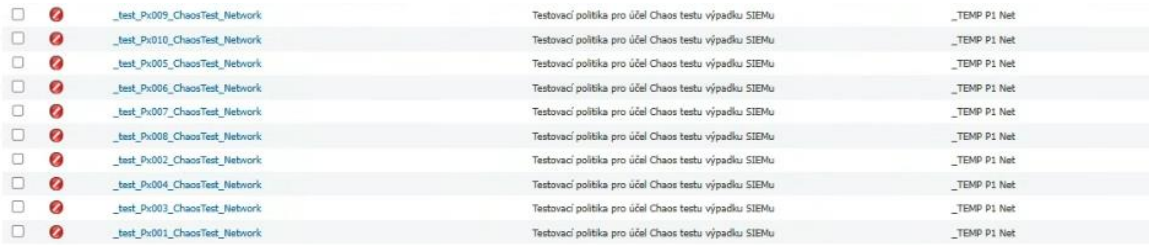
## 4.5 TC-02 Chaos test: výpadek toku z DLP do SIEM

Cílem tohoto scénáře je ověřit chování integrace při přibližně dvacetiminutové blokaci toku a následném obnovení přenosu, se zaměřením na ztráty, duplicity, chyby při parsování a mapování atribut a čas dohnání backlogu.

**Hypotéza pro TC-02**

Během dočasného přerušení přenosu mezi DLP a SIEM nedojde ke ztrátě ani neodůvodněné duplikaci testovacích událostí. Po obnovení toku systém backlog postupně zpracuje, zachová korektní parsování klíčových polí a v přiměřeném čase obnoví standardní režim zpracování událostí.

### 4.5.1 Příprava testovacích dat a systémů



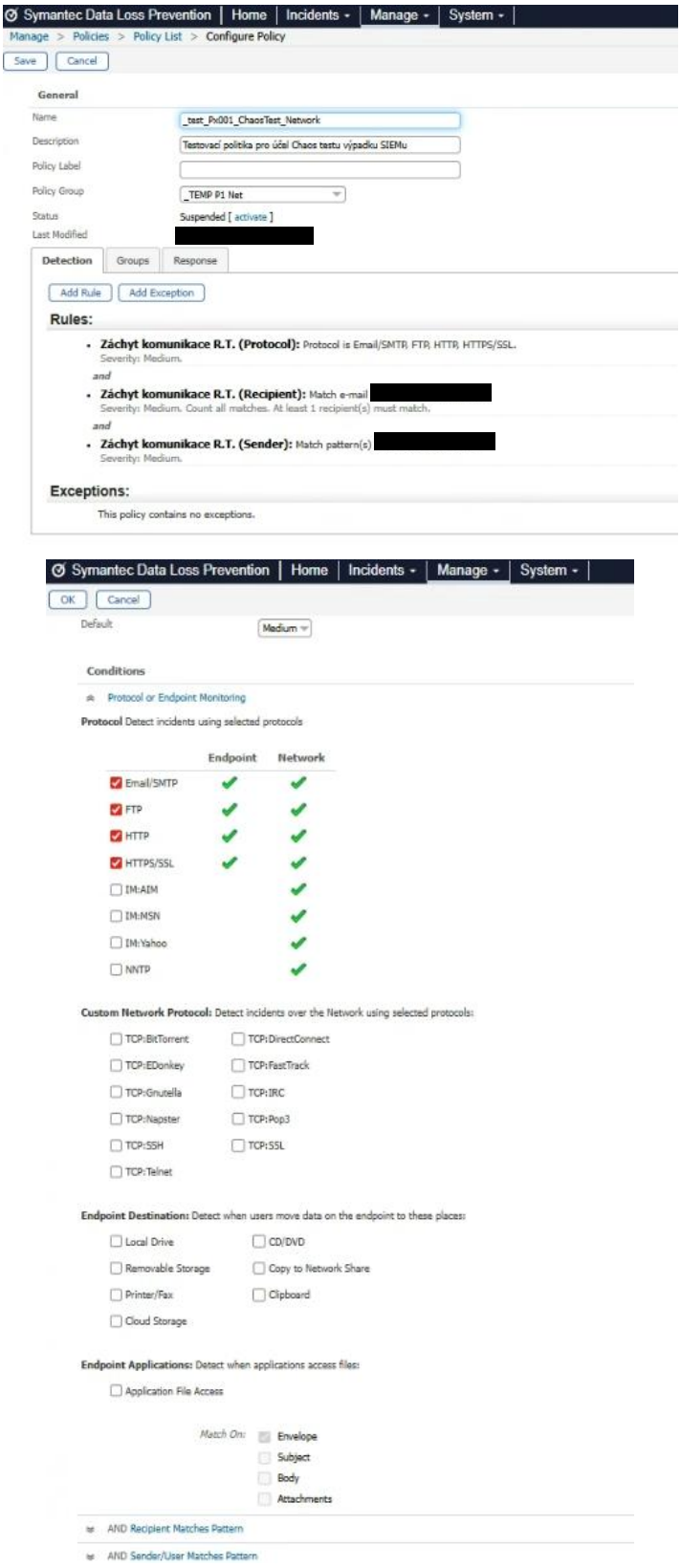

*Obrázek 20 - Seznam politik pro TC-02*

*Zdroj: (Vlastní zpracování)*

Stejně jako u předchozího scénáře byla pro scénář TC-02 připravena sada samostatných testovacích politika s cílem vygenerovat větší objem událostí pod jednotným názvem, aby bylo možné jednoznačně oddělit testovaný tok od ostatních provozních záznamů. Celkem se jednalo o 10 duplicitních politik s označením Px001 až Px010, jak je vidět na obrázku 20. Vytvoření duplicitních politik umožnilo snadno vygenerovat více záchytů naráz bez zbytečné časové zátěže. Plánovanou testovací sadou bylo 100 test eventů, vždy po deseti od každé politiky.

Pravidla pro spuštění záchytu byla obdobná jako u scénáře TC-01:

- Shoda protokolů: Vyhledávání probíhalo na protokolech FTP, Email/SMTP, HTTP a HTTPS/SSL
- Shoda příjemce: Aby došlo ke spuštění politiky, příjemcem musela být specifická e-mailová adresa. Zvolena byla soukromá e-mailová schránka.
- Shoda odesílatele: Aby došlo ke spuštění politiky, odesílatelem musela být specifická e-mailová adresa. Zvolen byl pracovní e-mail.




*Obrázek 21 - Testovací politika Px001*

*Zdroj: (Vlastní zpracování)*

Na obrázku 21 jsou zobrazeny detaily k volbě pravidel týkajících se protokolů. Symantec DLP sleduje protokoly, jak v rámci sítě, tak v rámci endpointu, pokud jsou na zařízení nainstalovány endpointové agenty. Kromě protokolů zvolených pro potřeby testu umožňuje DLP kontrolovat i další zdroje, například v rámci endpointu je schopné monitorovat přesun dat do:

- Místních i externích uložišť
- CD/DVD
- Cloudového uložiště
- Tiskárny nebo faxového zařízení
- Sdíleného místa v síti
- Clipboardu

Mimo přípravu politik bylo součástí systémové přípravy i průběžné monitorování provozu a chybovosti, aby test nevyvolal neočekávaný dopad na jiné zdroje nebo části produkční infrastruktury. Tato kontrola odpovídá stanoveným omezením a stop podmínkám testu, které mají zabránit tomu, aby experiment negativně ovlivnil běžný provoz mimo testovaný zdroj událostí.

### 4.5.2 Průběh testu

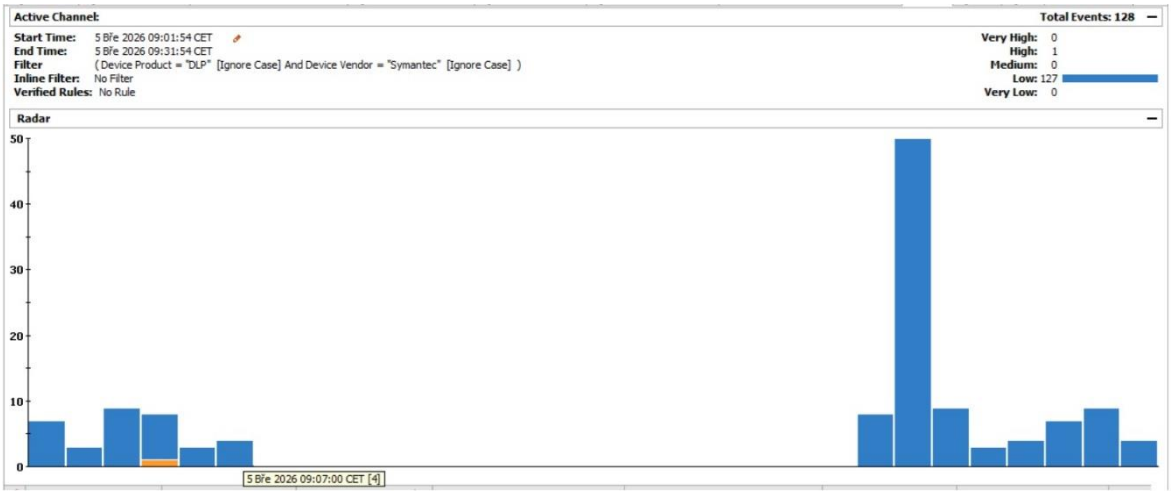
Po kontrole testovacích systémů byl dán pokyn k zastavení přenosu. Přenos událostí z DLP do SIEM byl zablokován na úrovni síťové komunikace v důsledku aplikace bezpečnostního pravidla firewallu, které v dané komunikační trase nepovolovalo odpovídající provoz. Z důvodu zachování bezpečnosti informací v podniku zde nejsou uváděny konkrétní síťové identifikátory.

Níže je uvedený časový rozpis (timeline) událostí sledovaných během blokace:

- ~9:03:00 – spuštění blokačního pravidla na úrovni firewall
- 9:05:17 – přerušení spojení na straně SIEM
- 9:06:53 – zpracování poslední zprávy v ESM Manager
- 9:10:00 – metodikům DLP dorazila výstraha, že nelze navázat spojení přes syslog
- 9:13:48-9:20:28 – vytvoření testovacích eventů
- ~9:20:00 – vypnutí blokačního pravidla na úrovni firewall
- 9:23:51 – poslední registrovaný blokovaný provoz na straně firewall
- 9:24:06 – navázání spojení na straně SIEM

Poznámka: Spuštění i zastavení pravidla firewall není instantní a může trvat až několik minut, než dojde ke změnám v datovém přenosu, proto jsou uvedené časy zapnutí a vypnutí pouze orientační a sledovaly se především odezvy systémů SIEM a DLP.

Po vypnutí blokačního pravidla se sledoval postupný návrat systémů do standardního režimu. Na obrázku 22 lze vidět výpadek provozu v ArcSight Console v okně radar, které poskytuje rychlý přehled o aktuálním stavu bezpečnosti systémů a sítě. Po opětovném napojení nastal velký nárůst záchytů, který ale systém rychle zpracoval a navrátil se do původního stavu.




*Obrázek 22 - ArcSight radar*

*Zdroj: (Vlastní zpracování)*

# 5 Výsledky

## 5.1 Výsledky TC-01

Vyhodnocení testů je založeno na porovnání exportů ze systému DLP a SIEM. U scénáře TC-01 je hlavním předmětem hodnocení úplnost doručení testovacích událostí, jejich dohledatelnost v SIEM a správnost parsování a mapování klíčových atributů. U každé testovací kategorie je sledováno, zda událost dorazila do konzole, zda nedošlo ke vzniku parsing error a zda nebyla chybně interpretována.

Ve výstupech DLP i v ESM Manager bylo dohledáno 7 zachycených a odeslaných/přijatých událostí. Úspěšný přenos byl potvrzený i skrze tcpdump. V tabulce 7 níže je uvedeno, kdy došlo k záchytům v jednotlivých komponentách integrace. Z uvedených dat vyplývá, že v rámci standardního přenosu je rozdíl doby zapsání eventu do systému DLP a do systému SIEM přibližně 30 sekund, v daném vzorku je konkrétně průměr 34,14 sekund. Zároveň lze pozorovat, že data jsou přenesena na SmartConnector už v okamžiku jejich zápisu do systému DLP.

| DLP Timestamp | Connector | SIEM | Politika_DLP |
|---|---|---|---|
| 10:30:55 | 10:30:55 | 10:31:21 | _test_Px303_\ suser="DATA\null" |
| 10:30:55 | 10:30:55 | 10:31:30 | _test_Px301_\ suser="DATA\jirackovver" |
| 10:30:55 | 10:30:55 | 10:31:30 | _test_Px302_\ suser="DATA\ňeexistuje" |
| 10:30:55 | 10:30:55 | 10:31:30 | _test_Px305_\ dvcpid=123456789 |
| 10:30:55 | 10:30:55 | 10:31:31 | _test_Px101_ParserTest_H_CEF:0\|SYMANTEC\|DLP\|CEF V0.1\|INCI |
| 10:30:55 | 10:30:55 | 10:31:31 | _test_Px304_\ msg=_test_Pxxx_Sandbox |
| 10:30:55 | 10:31:22 | 10:31:31 | _test_Px201_ParserTest_B_\ |

*Tabulka 7 - Časy záchytů TC-01*
*Zdroj: (Vlastní zpracování)*

Výsledky parsování a interpretace dat jsou uvedeny v tabulce 8, kde je zároveň barevně odlišeno, zda byla data zpracována bezchybně (zelená), s menšími chybami bez značného dopadu na související procesy (oranžová) nebo s podstatnými chybami (červená). Dále je proveden podrobný rozbor chyb v jednotlivých testovacích politikách

| Kategorie | Politika | Chyby parsování | Chybějící pole | Chyby v hodnotách |
|---|---|---|---|---|
| A | Px101 | Ano | Ne | Ano |
| A | Px201 | Ano | Ano | Ano |
| B | Px301 | Ano | Ne | Ne |
| B | Px302 | Ano | Ne | Ne |
| B | Px303 | Ano | Ne | Ano |

| | | | | |
|---|---|---|---|---|
| C | Px304 | Ano | Ne | Ne |
| C | Px305 | Ano | Ne | Ne |

*Tabulka 8 - Vyhodnocení TC-01*
*Zdroj: (Vlastní zpracování)*

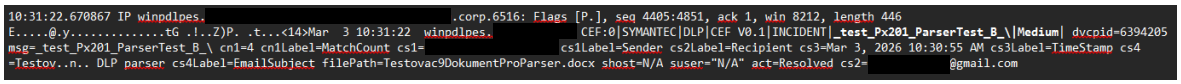
## Kategorie A

První kategorie politik se vyznačovala největší chybovostí, jelikož měla nejvýraznější dopady na rozdělení hlavičky CEF přenášených zpráv. Nicméně, u obou politik úspěšně proběhlo parsování a chyby se objevily pouze při zapisování hodnot do polí.

| Correla | Aggreg | Device Custom Strir | Devic | Device Ver | Message | Name | Priority | Severity |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | | DLP | SYMANTEC | | _test_Px201_ParserTest_B_\|Medium | 3 | 0 |
| 0 | 1 | 03.03.2026 10:30 | DLP | SYMANTEC | Testování DLP parser | _test_Px101_ParserTest_H_CEF:0 | 3 | 0 |

*Obrázek 23 - Hodnocení Kategorie A*
*Zdroj: (Vlastní zpracování)*

- Název politiky *_test_Px101_ParserTest_H_CEF:0|SYMANTEC|DLP|CEF V0.1|INCI* se při přepisu do systému SIEM zkrátil na *_test_Px101_ParserTest_H_CEF:0*. Zbytek názvu začínající prvním znakem | se namapoval jako pokračování hlavičky CEF. Parser byl i tak schopný korektně zpracovat zbytek zprávy, aniž by došlo k navazujícím chybám. Je ale potřeba zvážit, zda by tímto způsobem nemohlo například dojít k zásadním úpravám hlavičky, například ke kompletnímu přepsání některých polí.
- U druhé politiky se název naopak prodloužil z původního *_test_Px201_ParserTest_B_* na nový *_test_Px201_ParserTest_B_|Medium.* Jelikož původní název končil na únikový znak \, došlo k nechtěnému escapování prvního znaku | (obrázek 24) a přepsání pole se severitou „Medium“ na textový řetězec, který se stal součástí názvu politiky. Protože se předčasně ukončila hlavička CEF, nepodařilo se namapovat některá pole, jak je vidět na obrázku 23. Předčasné ukončení hlavičky CEF má tedy větší dopady než její umělé prodloužení.




*Obrázek 24 - tcpdump Px201*
*Zdroj: (Vlastní zpracování)*

## Kategorie B

V rámci Kategorie B proběhl pokus o injekci dvojice klíč=hodnota. Objevila se pouze jedna drobná chyba při interpretaci zprávy, která ale nesouvisela se samotnou injekcí. V tabulce 9 je zobrazeno srovnání hodnot, které byly součástí injekce, a správně interpretovaných hodnot.

| Politiks | Injekce | SIEM | Správná hodnota |
|---|---|---|---|
| Px301 | suser="DATA\jirackovver" | suser=„N/A“ | suser=„N/A“ |
| Px302 | suser="DATA\ňeexistuje" | suser=„N/A“ | suser=„N/A“ |
| Px303 | suser="DATA\null" | suser=„N/A“ | suser=„N/A“ |

*Tabulka 9 - Hodnocení Kategorie B*
*Zdroj: (Vlastní zpracování)*

Protože se v politice Px303 objevil řetězec \null a znak \ nebyl správně escapován, část textu se interpretovala jako speciální znak \n, který slouží k přechodu na další řádek. To vedlo ke změně názvu politiky na test_*Px303_\ suser="DATAull"*.

**Kategorie C**

Stejně jako u Kategorie B, ani zde nebyly pokusy o injekci úspěšné a data se správně parsovala i mapovala do polí. U politiky Px304 zůstal v poli „msg“ přepsaný název politiky a u politiky Px305 se správně namapovalo id zařízení (pro ověření bylo porovnáno s ostatními záchyty).

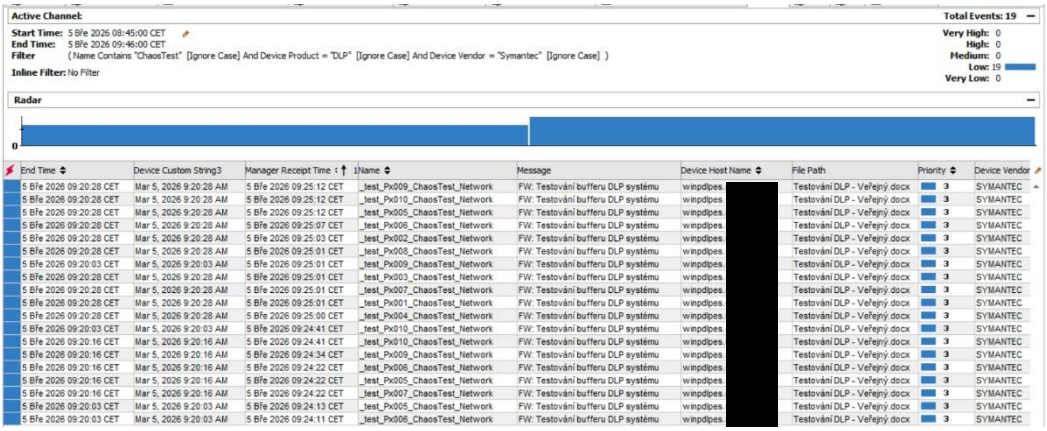
### 5.1.1 Shrnutí výsledků TC-01

Testovací scénář TC-01 ukázal, že standardní přenos událostí z DLP do ArcSight je funkční a události jsou dohledatelné, nicméně kvalita dat po zpracování v SIEM není ve všech případech bezchybná. Největší význam má zjištění, že nevhodně vložené speciální znaky v CEF hlavičce mohou změnit interpretaci zprávy, například dojde k nechtěnému zkrácení nebo naopak prodloužení hlavičky, což se následně projeví nesprávným zápisem hodnot do polí nebo chybějícími poli. Pro zkoumaný podnik to znamená, že i když událost do SIEM dorazí, může mít sníženou forenzní hodnotu a může dojít ke komplikacím při vyhodnocení incidentu v SOC. Současně testy injekcí ve formě klíč=hodnota ukázaly, že přímé přepsání polí tímto způsobem nebylo úspěšné, zde je tedy parsování a mapování dat odolné. V důsledku těchto zjištění byla hypotéza TC-01, stanovená v kapitole 4.4, zamítnuta.

## 5.2 Výsledky TC-02

U scénáře TC-02 je vyhodnocení rozšířeno o metriky související s výpadkem toku. Kromě úplnosti doručení a správnosti parsování se posuzoval zejména výskyt ztrát a duplicit a čas potřebný k dohnání backlogu po obnovení komunikace. Podstatné bylo také porovnání času vzniku události a času jejího příjmu v SIEM, které umožňuje určit, zda se systém po skončení blokace skutečně vrací do režimu blízkého real-time zpracování.

Exportem dat z konzole DLP bylo potvrzeno, že došlo k zachycení všech (100) plánovaných test eventů. Události byly zachytávány v „dávkách“ po deseti, vždy politiky Px001 až Px010, v souvislosti s tím, jak byly postupně odesílány e-maily, které aktivovaly záchyt. První dávka byla zachycena v 9:13:48 a poslední v 9:20:28.



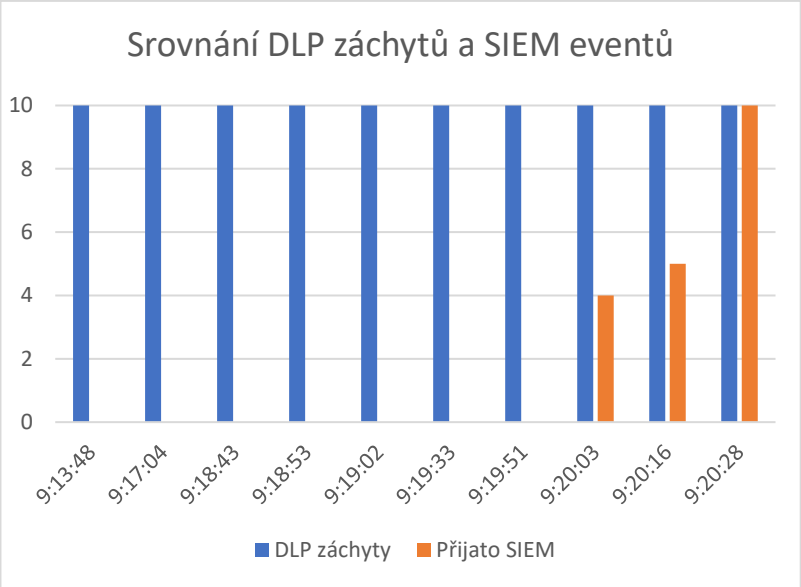

*Obrázek 25 - ArcSight Console TC-02*

*Zdroj: (Vlastní zpracování)*

Při srovnání s exportem SIEM bylo zjištěno, že do ESM Manageru dorazilo pouze 19 testovacích eventů ze 100 (lze vidět na obrázku 25).

Jednotlivé eventy jsou označeny parametrem cs3, tedy custom string 3, do kterého se mapuje časové razítko (Timestamp) záchytu v DLP. Tento parametr by neměl být ovlivněn časy přijetí do SIEM ani výpadkem. Do SIEM je odesíláno průměrně 4 až 10 DLP eventů za minutu a tento rozsah by měl zůstat konzistentní i v rámci výpadku, což nám umožňují sledovat právě časová razítka eventů. Při analýze výsledného exportu bylo ale zjištěno, že do SIEM dorazil event s Timestamp 9:07:16 a následující až s Timestamp 9:20:03. Objevilo se tedy hluché místo trvající 12 minut 47 sekund, během kterého nebyly poslané žádné eventy z DLP do SIEM, a to ani dodatečně po opětovném navázání spojení.

Kontrolou výstupu tcpdump se potvrdilo, že záchyty se v hluchém místě nepřeposlaly ani na Connector, problém tedy nastal už přímo v DLP, odkud se po ukončení výpadku odeslala pouze malá část testovacích událostí.




*Graf 5 - Srovnání DLP záchytů a SIEM eventů*

*Zdroj: (Vlastní zpracování)*

Při analýze konkrétních eventů (resp. dávek eventů), které se podařilo přenést do SIEM, jak je zobrazeno v grafu 5, lze vidět, že kompletně se odeslala pouze poslední dávka 10 eventů v 9:20:28, dále 5 záchytů z předposlední dávky v 9:20:16 a 4 záchyty z 8. dávky v 9:20:03.

| DLP Timestamp | Connector | SIEM | Dávka | Politiks |
|---|---|---|---|---|
| 9:20:03 | 9:20:03 | 9:24:11 | 8. | _test_Px006_ChaosTest_Network |
| 9:20:03 | 9:20:03 | 9:24:13 | 8. | _test_Px005_ChaosTest_Network |
| 9:20:03 | 9:20:03 | 9:24:41 | 8. | _test_Px010_ChaosTest_Network |
| 9:20:03 | 9:20:03 | 9:25:01 | 8. | _test_Px009_ChaosTest_Network |
| 9:20:16 | 9:20:16 | 9:24:22 | 9. | _test_Px007_ChaosTest_Network |
| 9:20:16 | 9:20:16 | 9:24:22 | 9. | _test_Px006_ChaosTest_Network |
| 9:20:16 | 9:20:16 | 9:24:22 | 9. | _test_Px005_ChaosTest_Network |
| 9:20:16 | 9:20:16 | 9:24:41 | 9. | _test_Px010_ChaosTest_Network |
| 9:20:16 | 9:20:16 | 9:24:34 | 9. | _test_Px009_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:01 | 10. | _test_Px001_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:01 | 10. | _test_Px003_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:00 | 10. | _test_Px004_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:03 | 10. | _test_Px002_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:01 | 10. | _test_Px008_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:01 | 10. | _test_Px007_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:07 | 10. | _test_Px006_ChaosTest_Network |

| | | | | |
|---|---|---|---|---|
| 9:20:28 | 9:20:28 | 9:25:12 | 10. | _test_Px005_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:12 | 10. | _test_Px010_ChaosTest_Network |
| 9:20:28 | 9:20:28 | 9:25:12 | 10. | _test_Px009_ChaosTest_Network |

*Tabulka 10 - Přehled přenesených eventů*
*Zdroj: (Vlastní zpracování)*

V tabulce 10 jsou uvedeny následující hodnoty:

- DLP Timestamp: Kdy vznikly záchyty v systému DLP
- Connector: Kdy byly eventy přeposlány do Connectoru
- SIEM: Kdy se eventy zalogovaly do ESM Manageru
- Dávka: Do kolikáté dávky záchyty patřily
- Politika: O jakou konkrétní politiku se jednalo

Pokud bereme v potaz dobu navázání spojení se SIEM, která byla 9:24:06 (dle informací ze systému), trvalo platformě 1 min 6 s zpracovat 19 eventů přijatých během výpadku. První event navazující na přerušení provozu se logoval v 9:24:11 (8. dávka, politika _test_Px_006_ChaosTest_Network), 5 s po opětovném navázání spojení v SIEM a 4 min 8 s po vzniku záchytu v DLP. Poslední event byl registrován v 9:25:12 (10. dávka, _test_Px009_ChaosTest_Network), 1 min 6 s po spojení a 4 min 44 s po vzniku záchytu. Nevznikly žádné duplicity.

| | |
|---|---|
| **Počet poslaných** | 100 eventů |
| **Počet přijatých** | 19 eventů |
| **Ztracené eventy** | 81 eventů |
| **Duplicity** | 0 eventů |
| **Eventy s chybějícími poli** | 11 eventů |
| **Doba zpracování v SIEM** | 1 min 1 s |
| **D. z. po navázání spojení MIN** | 5 s |
| **D. z. po navázání spojení MAX** | 1 min 6 s |
| **D. z. po navázání spojení PRŮMĚR** | 42 s |

*Tabulka 11 - Přehled parametrů TC-02*
*Zdroj: (Vlastní zpracování)*

### 5.2.1 Shrnutí výsledků TC-02

Scénář TC-02 poukázal na problémy zejména z hlediska spolehlivosti a odolnosti. Test ukázal, že po dočasném přerušení datového toku se sice po obnovení komunikace přenos opět rozběhne a ArcSight je schopný přijaté události rychle zpracovat, ale zároveň nedošlo k dodatečnému zpracování většiny (81 %) událostí, které vznikly během výpadku. Analýza potvrdila, že problém nevznikl až v SIEM nebo na konektoru, ale už na straně DLP, jelikož

se události z hluchého místa po obnově spojení vůbec nepřeposlaly. Pro zkoumaný podnik to může znamenat, že v případě obdobného výpadku může vzniknout reálné slepé místo v monitoringu, kdy SOC nebude mít v SIEM kompletní obraz o DLP incidentech v daném časovém okně. Pozitivní zjištění je, že u přenesené části nevznikly duplicity, tedy po obnově toku nedochází k zahlcení SOC opakovanými událostmi. Hypotéza TC-02 byla tímto výsledkem vyvrácena, protože předpoklad „bez ztrát po obnově toku“ se nepotvrdil.

## 5.3 Doporučení podniku

Níže jsou uvedeny doporučení pro zkoumaný podnik vycházející z výsledků obou testovacích scénářů. U TC-01 jsou zaměřena na standardizaci pojmenování politik a u TC-02 je vytvořen scénář reakce na výpadek, který reflektuje zjištěné informace z testů.

### 5.3.1 Doporučení v návaznosti na TC-01

Na základě výsledků scénáře TC-01 lze jako nejefektivnější opatření doporučit sjednocení způsobu pojmenovávání DLP politik, protože právě název politiky má největší dopad na formát CEF. Zavedení jednotných pravidel pojmenování by zároveň mělo přínos v podobě lepší dohledatelnosti a snazší tvorby reportů, aniž by bylo nutné zasahovat do samotné integrační architektury.

Názvy politik by měly:

- mít pevnou strukturu, např. _<SPOLEČNOST>_<ID>_<NÁZEV>_<KANÁL>
- obsahovat kanál (zpravidla Network / Endpoint)
- mít unikátní ID pro dohledání změn a reporty
- používat jednotný jazyk a jednotné zkratky
- být krátké a čitelné, aby se zobrazovaly celé v konzolích a reportech

Názvy politik by neměly:

- obsahovat speciální znaky, zejména |, \, =, uvozovky a znaky nového řádku
- používat diakritiku a nestrukturovaný text
- být měněny bez zaevidování informace, že dochází ke změně v názvu – (kvůli návaznosti v SIEM a reportech)
- používat více různých názvů pro stejný typ detekce

### 5.3.2 Doporučení v návaznosti na TC-02

Výsledky TC-02 ukázaly, že při výpadku toku může vzniknout reálné slepé místo v SIEM, které se po obnovení komunikace samo nedoplní o přeskočené události. Aby byl minimalizován případný dopad, byl podniku doporučen scénář, jak postupovat, pokud by skutečně došlo k dočasnému přerušení provozu mezi DLP a SIEM.

| Název: | Výpadek přenosu ze Symantec DLP do ArcSight SIEM |
|---|---|
| Dotčené uživatelské skupiny: | • Metodici DLP<br>• Analytici SOC<br>• Operátoři SOC |
| Cíl: | Vymezení dopadu přerušení spojení (hluchého místa), identifikace dotčených bezpečnostních politik a doplnění ztracených událostí do SIEM |
| Trigger: | Přerušení spojení mezi Symantec DLP a ArcSight SIEM |
| Instrukce: | 1. <u>Detekce a eskalace</u><br>a. Analytici SOC zaznamenají anomálii (absence eventů DLP, systémové varování),<br>• provedou rychlou validaci například pomocí filtru na DLP zdroj a<br>• neprodleně informují metodiky DLP.<br>• Metodici DLP ověří, zda DLP události vznikají (není chyba na straně DLP).<br>b. Metodici DLP zaznamenají anomálii (systémové varování) a<br>• ověří, že DLP události vznikají (není chyba na straně DLP) a<br>• neprodleně informují analytiky SOC.<br>• Analytici SOC provedou rychlou validaci, zda je tok skutečně přerušen.<br>2. <u>Logování časů</u><br>• Operátoři SOC založí výpadek jako incident skrze interní požadavkový systém<br>• Do incidentu se zapisují klíčové časy:<br>o Čas detekce výpadku<br>o Začátek výpadku (odhad podle poslední zpracované události v SIEM – parametr cs3 – Timestamp)<br>o Konec výpadku (odhad podle první zpracované události v SIEM po opětovném navázání spojení)<br>o Stabilizace (konzistentní běh toku)<br>3. <u>Vymezení dopadu</u><br>• Analytici SOC provedou export událostí začínající těsně (±5 min) před odhadovaným začátkem výpadku a končící se stabilizací běhu toku. |

| | |
|---|---|
| | • Na základě parametru cs3 vymezí přesné časové okno v intervalu <Timestamp poslední DLP události před výpadkem, Timestamp první DLP události po obnovení><br>4. Přeposlání chybějících eventů<br>• Metodici DLP v DLP konzoli vyfiltrují všechny záchyty v určeném časovém okně.<br>• Zajistí manuální zaslání vyfiltrované sady do SIEM (případně jako export v csv).<br>• Analytici SOC ověří, že se doplněné události objevily v ArcSight.<br>5. Uzavření incidentu<br>• Operátoři SOC doplní do incidentu<br>o Potvrzené časové okno výpadku<br>o Zda bylo možné události částečně / kompletně doplnit |
| Poznámka: | Tímto scénářem se řeší pouze doplnění chybějících záchytů, příčina výpadku a zajištění obnovy provozu se řeší separátně. |

*Tabulka 12 - Scénář pro výpadek přenosu*
*Zdroj: (Vlastní zpracování)*

# 6 Závěr

Cílem této diplomové práce bylo analyzovat a vyhodnotit integraci systému pro prevenci úniku dat DLP a systému pro správu bezpečnostních událostí SIEM se zaměřením na spolehlivost, rychlost a kvalitu přenosu dat mezi systémy a na základě zjištění navrhnout doporučení pro zkoumaný podnik.

V teoretické části byly nejprve shrnuty důležité koncepty podnikové informační bezpečnosti včetně přehledu kybernetických hrozeb, mezinárodních standardů a legislativních požadavků. Pozornost byla věnována především principům fungování systémům DLP a SIEM, zejména jejich architektuře a metodám detekce. Zároveň bylo nahlédnuto na problematiku integrace bezpečnostních systémů, způsoby přenosů dat mezi nimi a typickým problémům, které při integraci vznikají.

Praktická část navázala na teoretická východiska analýzou integrace Symantec DLP a ArcSight SIEM v reálném prostředí zkoumaného podniku. Byla popsána současná integrační architektura včetně role komponent zajišťující přenos bezpečnostních událostí a jejich zpracování v ArcSight. V návaznosti na tuto analýzu byly navrženy a realizovány dva testovací scénáře. První scénář TC-01 ověřoval kvalitu dat při standardním provozu se zaměřením na parsování a správnost mapování klíčových atribut ve struktuře CEF. Druhý scénář TC-02 byl pojat jako chaos test, při kterém bylo simulováno dočasné přerušení datového toku mezi DLP a SIEM za účelem ověření odolnosti integrace. Během testu bylo v rámci výpadku odesláno předem dané množství testovacích událostí a sledovalo se chování systému po obnovení komunikace. Omezením byla skutečnost, že testování probíhalo na menším vzorku testovacích dat, což vyplývalo mimo jiné z provozních a personálních omezení v prostředí podniku a z nutnosti nezasahovat do produkčního provozu.

U scénáře TC-01 se ukázalo, že nevhodně vložené znaky v polích, která se následně mapují do hlavičky CEF, mohou ovlivnit interpretaci zprávy a vést k nechtěné modifikaci hlavičky, což se projeví nesprávným zápisem hodnot do polí nebo přímo chybějícími údaji. To pro zkoumaný podnik znamená, že i při úspěšném doručení události může mít záznam v SIEM sníženou forenzní hodnotu a může komplikovat vyhodnocení incidentu v SOC. Zároveň se ukázalo, že pokusy o injekci dat ve formě klíč=hodnota byly neúspěšné a nejedná se v tomto případě o hrozbu.

Scénář TC-02 ukázal především na provozní rizika spojená se spolehlivostí a odolností integrace. Test prokázal, že po obnovení komunikace po výpadku se sice tok událostí rychle vrátí do režimu blízkého real-time, ale nedošlo k dodatečnému zpracování většiny událostí vzniklých během výpadku, které zůstaly v backlogu DLP. Problém byl identifikován právě na straně DLP, kde vznikl časový interval, z kterého se po obnově spojení testovací události nepřeposlaly. Pro podnik to znamená riziko vzniku hluchého místa v monitoringu, kdy SOC nemusí mít v SIEM kompletní obraz o DLP incidentech v daném časovém úseku.

Na základě výsledků byla formulována doporučení pro zkoumaný podnik. V návaznosti TC-01 bylo doporučeno zavést jednotná pravidla pro pojmenovávání

DLP politik, protože název politiky má v dané implementaci významný dopad na interpretaci formátu CEF a zároveň ovlivňuje dohledatelnost a reportování událostí v SIEM. Zároveň byla doporučena konkrétní pravidla povolených a zakázaných způsobů pojmenování politik. V návaznosti na TC-02 byl navržen scénář reakce na výpadek toku, který zahrnuje zajištění informovanosti všech interesovaných stran, logování podstatných informací vznikajících během výpadku, vymezení konkrétního časového okna, kdy vzniká hluché místo, a následné manuální doplnění chybějících záchytů ze strany DLP do SIEM.

# 7 Seznam použitých zdrojů


ALI, Muhammad, 2025. What is syslog? *LogicMonitor* [online]. Available at: https://www.logicmonitor.com/blog/what-is-syslog

ATLASSIAN, 2025. Webhooks. *developer.atlassian.com* [online]. Available at: https://developer.atlassian.com/cloud/jira/platform/webhooks/#overview

BARTLEY, Kevin, 2025. Big data statistics: How much data is there in the world? *Rivery* [online]. Available at: https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/

BHATT, Sandeep, Pratyusa K. MANADHATA and Loai ZOMLOT, 2014. The operational role of security information and event management systems. *IEEE Security & Privacy* [online]. **12**(5), 35–41. Available at: doi:10.1109/msp.2014.103

BROOKS, Charles J., Christopher GROW, Philip A. CRAIG Jr and Donald SHORT, 2018. *Cybersecurity Essentials*. B.m.: John Wiley & Sons.

BURGE, Paul, Tyler O'CONNOR and Ross ROBERTSON, 2022. *Social engineering & cybercrime remain top cyber insurance concerns - Tools and Intel | CRC Specialty* [online]. Available at: https://www.crcgroup.com/Tools-and-Intel/post/social-engineering-cybercrime-remain-top-cyber-insurance-concerns

CHOPRA, Meenu and Cosmena MAHAPATRA, 2019. Significance of Security Information and Event Management (SIEM) in modern Organizations. *International Journal of Innovative Technology and Exploring Engineering* [online]. **8**(7S2), 432–435. Available at: https://www.ijitee.org/wp-content/uploads/papers/v8i7s2/G10740587S219.pdf

CLOUDFLARE, 2025. What is encryption? *Cloudflare* [online]. Available at: https://www.cloudflare.com/learning/ssl/what-is-encryption/

DE SOUSA, Edson Machado and Abid SHAHZAD, 2021. Data Loss Prevention from a Malicious Insider. *Journal of Computer Information Systems* [online]. **62**(6), 1101–1111. Available at: doi:10.1080/08874417.2021.1980748

ELASTIC, 2025. winlog input. *elastic.co* [online]. Available at: https://www.elastic.co/docs/reference/beats/filebeat/filebeat-input-winlog

EUROPEAN COMMISSION, 2025. NIS2 Directive: securing network and information systems. *Shaping Europe's Digital Future* [online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

FAIZ, Mohamed Falah, Junaid ARSHAD, Mamoun ALAZAB and Andrii SHALAGINOV, 2019. Predicting likelihood of legitimate data loss in email DLP. *Future Generation Computer Systems* [online]. **110**, 744–757. Available at: doi:10.1016/j.future.2019.11.004

GEEKSFORGEEKS, 2025. Difference between Antivirus and Antimalware. *GeeksforGeeks* [online]. Available at: https://www.geeksforgeeks.org/computer-networks/difference-between-antivirus-and-antimalware/

GHELANI, Diptiben, 2023. Securing the Future: Exploring the Convergence of Cybersecurity, Artificial Intelligence, and Advanced Technology. *International Journal of Computer Trends and Technology* [online]. **71**(10), 39–44. Available at: doi:10.14445/22312803/ijctt-v71i10p105

GHILLIONE, Daniel, 2024. What Are Computer Worms? *LevelBlue* [online]. Available at: https://levelblue.com/blogs/levelblue-blog/what-are-computer-worms

GONZÁLEZ-GRANADILLO, Gustavo, Susana GONZÁLEZ-ZARZOSA and Rodrigo DIAZ, 2021. Security Information and Event Management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors* [online]. **21**(14), 4759. Available at: doi:10.3390/s21144759

HARIHARASUBRAMANIAN, Neeraja, 2025. What is SOC? An Essential Guide to Security Operations Centers. *Fidelis Security* [online]. Available at: https://fidelissecurity.com/cybersecurity-101/learn/what-is-soc-security-operations-center/

HISCOX, 2025. *Hiscox Cyber Readiness Report 2025* [online]. Available at: https://www.hiscoxgroup.com/sites/group/files/documents/2025-10/HSX374%20%E2%80%93%202025%20CRR%20Report%20Final.pdf

HUNTERS, 2025. *Microsoft Windows Event Logs* [online]. Available at: https://docs.hunters.ai/docs/microsoft-windows-event-logs

HURALNYK, Oleksandr, Andrzej KWIECIEN, Vadym PAIUK, Olexandr KLEIN and Oleksii LYHUN, 2025. Method and Means of Critical Information Processing in Corporate Networks. *IntelITSIS 2025* [online]. 314–328. Available at: https://ceur-ws.org/Vol-3963/paper25.pdf

IAVICH, Maksim, Giorgi AKHALAIA, Roman ODARCHENKO and Ana IMNADZE, eds., 2024. Fortifying the digital fortress: A multi-layered defense strategy with SIEM, mail gateway, and sandbox technologies. *International Workshop on Algorithms of Data Processing* [online]. 216–226. Available at: https://ceur-ws.org/Vol-3895/paper18.pdf

IBM CORPORATION, 2022. *Cost of a Data Breach Report 2022* [online]. Available at: https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf

INFO-TECH RESEARCH GROUP, 2025. Select and Implement a SIEM Solution. *Info-Tech* [online]. Available at: https://www.infotech.com/workshops/select-and-implement-a-siem-solution

JARRETT, Andrew, 2025. Defending the digital perimeter: Modern Cybersecurity for SOC. *Cybersecurity Exchange* [online]. Available at: https://www.eccouncil.org/cybersecurity-exchange/security-operation-center/modern-cybersecurity-for-soc/

KHALIL, Mohammed, 2025. Dark Web Data Pricing 2025: Real costs of stolen data & services. *DeepStrike* [online]. Available at: https://deepstrike.io/blog/dark-web-data-pricing-2025

KORET, Joxean and Elias BACHAALANY, 2015. *The antivirus Hacker's handbook* [online]. Available at: doi:10.1002/9781119183525

KOTENKO, Igor, Andrey CHECHULIN and Evgenia NOVIKOVA, 2012. Attack Modelling and Security Evaluation for Security Information and Event Management. [online]. 391–394. Available at: doi:10.5220/0004063403910394

KOVÁŘ, Dalibor a Pavel AMLER, 2021. Už jste slyšeli o nařízení eIDAS 2.0. *EPRAVO.CZ* [online]. Available at: https://www.epravo.cz/top/clanky/uz-jste-slyseli-o-narizeni-eidas-20-113866.html

KYRIAZOGLOU, John, 2024. *Information Security incident and Data breach management* [online]. Available at: doi:10.1007/979-8-8688-0870-8

MARKOS, Ereni, Priscilla PEÑA, Lauren I. LABRECQUE and Kunal SWANI, 2023. Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *Journal of Consumer Affairs* [online]. **57**(3), 1089–1119. Available at: doi:10.1111/joca.12554

MUHAMMAD, Adabi Raihan, Parman SUKARNO and Aulia Arif WARDANA, 2023. Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science* [online]. **217**, 1406–1415. Available at: doi:10.1016/j.procs.2022.12.339

OPEN TEXT, 2023. *ArcSight SmartConnectors: Implementing ArcSight Common Event Format (CEF) - Version 26* [online]. Available

at: https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors-8.4/pdfdoc/cef-implementation-standard/cef-implementation-standard.pdf

OPEN TEXT CORPORATION, 2025. *ESM 101* [online]. Available at: https://www.microfocus.com/documentation/arcsight/arcsight-esm-7.9/pdfdoc/ESM_101/ESM_101.pdf

PODZINS, Oskars and Andrejs ROMANOVS, 2019. Why SIEM is Irreplaceable in a Secure IT Environment? *Conference: 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)* [online]. 1–5. Available at: doi:10.1109/estream.2019.8732173

PULYALA, Srinivas Reddy, 2024. From detection to prediction: AI-powered SIEM for proactive threat hunting and risk mitigation. *Türk Bilgisayar Ve Matematik Eğitimi Dergisi* [online]. **15**(1), 34–43. Available at: doi:10.61841/turcomat.v15i1.14393

RAJU, Steffi, 2016. Enhancing Security Information and Event Management to Develop Future-Ready Security Operations Center. *International Journal of Engineering and Technical Research* [online]. **5**(4), 46–50. Available at: https://www.erpublication.org/published_paper/IJETR042329.pdf

ROMANOSKY, Sasha, David HOFFMAN and Alessandro ACQUISTI, 2014. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies* [online]. **11**(1), 74–104. Available at: doi:10.1111/jels.12035

RUOHONEN, Jukka, Kalle HJERPPE, Jukka RUOHONEN and Kalle HJERPPE, 2021. The GDPR enforcement fines at glance. *Information Systems* [online]. **106**, 101876. Available at: doi:10.1016/j.is.2021.101876

SACHENKO, Anatoliy, Petro VIZHEVSKYI, Oleg SAVENKO, Viktor OSTROVERKHOV and Bogdan MASLYYAK, 2025. Modern strategies for data leak detection and prevention in corporate networks. *Modern Data Science Technologies Doctoral Consortium* [online]. 275–292. Available at: https://ceur-ws.org/Vol-4005/paper19.pdf

SEARCHINFORM, 2025. Maximizing Security with DLP and SIEM Integration - SearchInform. *SearchInform.com* [online]. Available at: https://searchinform.com/articles/cybersecurity/measures/dlp/deployment/dlp-and-siem-integration/

SECUREWORKS, 2024. History of Intrusion Detection & Prevention. *Secureworks* [online]. Available at: https://www.secureworks.com/blog/the-evolution-of-intrusion-detection-prevention

SENTINELONE, 2025. What is SIEM Architecture? Components & Best Practices. *SentinelOne* [online]. Available at: https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-architecture/

SINGH, Rahul, 2024. What is Symantec Data Loss Prevention and use cases of Symantec Data Loss Prevention? - DevOpsSchool.com. *DevOpsSchool.com* [online]. Available at: https://www.devopsschool.com/blog/what-is-symantec-data-loss-prevention-and-use-cases-of-symantec-data-loss-prevention/

SKRUNDA, Alexa, 2025. Integrating Firewalls with SIEM: Enhancing Threat Detection and Response -. *OutsourceITsecurity.com* [online]. Available at: https://outsourceitsecurity.com/integrating-firewalls-with-siem-enhancing-threat-detection-and-response

TENCENT CLOUD, 2025. How to integrate the office security platform with the SIEM system? *Tencent Cloud* [online]. Available at: https://www.tencentcloud.com/techpedia/123428

THE NIS2 DIRECTIVE, 2023. NIS2 Requirements | 10 Minimum measures to address. *The NIS2 Directive* [online]. Available at: https://nis2directive.eu/nis2-requirements/

UETZ, Rafael, Marco HERZOG, Louis HACKLÄNDER, Simon SCHWARZ and Martin HENZE, 2023. You Cannot Escape me: Detecting evasions of SIEM rules in enterprise networks. *arXiv (Cornell University)* [online]. Available at: doi:10.48550/arxiv.2311.10197

VERIZON, 2008. *Verizon 2008 Data Breach Investigations Report* [online]. Available at: https://www.verizon.com/business/resources/reports/databreachreport.pdf

VERIZON, 2022. *Verizon 2022 Data Breach Investigations Report* [online]. Available at: https://www.verizon.com/business/resources/reports/2022-dbir-data-breach-investigations-report.pdf

VERIZON, 2024. *Verizon 2024 Data Breach Investigations Report* [online]. Available at: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

WARREN, Tom, 2025. Microsoft is moving antivirus providers out of the Windows kernel. *The Verge* [online]. Available at: https://www.theverge.com/news/692637/microsoft-windows-kernel-antivirus-changes

# Seznam obrázků, tabulek, grafů a zkratek

## 7.1 Seznam obrázků

Obrázek 1 - Architektura systému SIEM ..... 32
Obrázek 2 - Architektura Hierarchical Managers modelu ..... 34
Obrázek 3 - Model metody Adaptive Misuse Detection ..... 35
Obrázek 4 - Integrovaná architektura Botnet Detection a DLP ..... 42
Obrázek 5 - Integrace systémů SIEM a IDS ..... 43
Obrázek 6 - Vzorový strom pro experimenty založené na rozhodovacím stromu ..... 44
Obrázek 7 - Architektura Symantec DLP ..... 48
Obrázek 8 - Pravidla politiky pro ochranu obchodního tajemství ..... 51
Obrázek 9 - Architektura ArcSight Enterprise Security Management ..... 53
Obrázek 10 - Komponentový UML diagram přenosu dat z DLP do SIEM ..... 56
Obrázek 11 - Seznam politik pro TC-01 ..... 58
Obrázek 12 - Testovací politiky Px101 a Px201 ..... 59
Obrázek 13 - Pravidla testovací politiky Px101 ..... 60
Obrázek 14 - Testovací politika Px303 ..... 61
Obrázek 15 - Atribut suser ..... 61
Obrázek 16 - Testovací politika Px304 ..... 62
Obrázek 17 - Testovací politika Px401 ..... 63
Obrázek 18 - Kontrola tcpdump ..... 64
Obrázek 19 - ArcSight Console TC-01 ..... 64
Obrázek 20 - Seznam politik pro TC-02 ..... 65
Obrázek 21 - Testovací politika Px001 ..... 66
Obrázek 22 - ArcSight radar ..... 68
Obrázek 23 - Hodnocení Kategorie A ..... 70
Obrázek 24 - tcpdump Px201 ..... 70
Obrázek 25 - ArcSight Console TC-02 ..... 72

## 7.2 Seznam tabulek

Tabulka 1 - Klasifikace DLP systémů podle modelu nasazení ..... 27
Tabulka 2 - Klasifikace DLP systémů podle koncepčního přístupu ..... 28
Tabulka 3 - Nejlépe hodnocené DLP systémy k roku 2025 ..... 29
Tabulka 4 - Nejlépe hodnocené SIEM systémy k roku 2025 ..... 37
Tabulka 5 - Testovací scénáře ..... 57
Tabulka 6 - Seznam politik pro TC-01 ..... 58
Tabulka 7 - Časy záchytů TC-01 ..... 69
Tabulka 8 - Vyhodnocení TC-01 ..... 70
Tabulka 9 - Hodnocení Kategorie B ..... 71

Tabulka 10 - Přehled přenesených eventů ..... 74
Tabulka 11 - Přehled parametrů TC-02 ..... 74
Tabulka 12 - Scénář pro výpadek přenosu ..... 77

## 7.3 Seznam grafů

Graf 1 - Nárůst Ransomware útoků mezi lety 2018 až 2024 ..... 15
Graf 2 - Bezpečnostní incidenty způsobené neúmyslným chováním interních aktérů ..... 17
Graf 3 - Vyřešené a zamítnuté soudní spory týkající se porušení ochrany osobních údajů v letech 2000 až 2011 ..... 21
Graf 4 - Vývoj záchytů pro bezpečnostní politiku OT ..... 52
Graf 5 - Srovnání DLP záchytů a SIEM eventů ..... 73