Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Výběr a nasazení EDR řešení v korporátním prostředí

Jakub Veber

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jakub Veber

Informatika

Název práce

Výběr a nasazení EDR řešení v korporátním prostředí

Název anglicky

Selection and Implementation of EDR Solution in Corporate Environment

---

Cíle práce

Cílem práce je popsání současné situace v kyberbezpečnosti a hrozbách, kterým firmy čelí, jak je možné se proti těmto hrozbám bránit pomocí antivirových, EDR a XDR řešení, porovnání těchto řešení a popsání best practice pro výběr tohoto řešení. V praktické části popsání reálného výběru a nasazení EDR řešení v korporátním prostředí a porovnání s best practice.

Metodika

V rámci BP bude v teoretické části popsáno, co je to EDR, rozdíly mezi klasickými antiviry, EDR a XDR. Jednotlivé výhody a nevýhody, jaké jsou současné bezpečnostní hrozby a jak tyto nástroje mohou firmám pomoci se jim bránit. Dále bude popsáno, jaké jsou best practice pro nasazení EDR a jejich místo v in-depth security a layered security. V praktické části budou řešeny samotné požadavky pro výběrové řízení, předvýběr kandidátů, POC, výběr a samotné nasazení ve zvolené společnosti a porovnání reálného nasazení s best practice.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

EDR, XDR, antivirus, cybersecurity, kyberbezpečnost

Doporučené zdroje informací

Cybersecurity – Attack and Defense Strategies – Second Edition, Yuri Diogenes , Dr. Erdal Ozkaya, ISBN 9781838827793
Cybersecurity Blue Team Toolkit, Nadean H. Tanner, ISBN 9781119552932
Cybersecurity Threats, Malware Trends, and Strategies, Tim Rains, ISBN 9781800206014

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. David Buchtela, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 28. 11. 2023

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 9. 2. 2024

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 25. 02. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Výběr a nasazení EDR řešení v korporátním prostředí" jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 13.03.2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Davidu Buchtelovi, Ph.D. za poskytnutí cenných rad a za odborné vedení této práce.

Výběr a nasazení EDR řešení v korporátním prostředí

Abstrakt

Tato práce je zaměřena na současnou situaci v kybernetické bezpečnosti a nejčastější kybernetické hrozby, kterým firmy čelí. Dále jsou popsány antivirová, Endpoint Detection and Response, eXtended Detection and Response řešení. Práce dále rozebírá, jak jednotlivá řešení pomáhají firmy chránit před nejčastějšími hrozbami a porovnává jednotlivá řešení. Také popisuje osvědčené postupy pro výběr a nasazení EDR řešení a zasazení tohoto řešení do modelu Defence in Depth.

Vlastní práce se věnuje popisu stávajícího prostředí Společnosti, průběhu výběrového řízení od definování technických požadavků, přes jednotlivá kola výběrového řízení až po konečný výběr EDR řešení. Následně práce popisuje samotný proces nasazení vybraného EDR řešení v prostředí Společnosti.

Dalším cílem této práce je porovnání reálného výběru a nasazení v prostředí Společnosti s osvědčenými postupy.

Klíčová slova: EDR, XDR, antivirus, korporátní prostředí, kybernetická bezpečnost, malware, defence in-depth, layered security, best practice, výběrové řízení

Selection and Implementation of EDR Solution in Corporate Environment

Abstract

This bachelor thesis focuses on the current situation in cyber security, the most common cyber threats that companies face. Antivirus, Endpoint Detection and Response, eXtended Detection and Response solutions are also described. Thesis also discusses how each solution helps companies protect against the most common threats and compares the solutions. Thesis also describes best practices for selecting and deploying an EDR solution and how this solution fits into the Defence in Depth model.

Thesis itself describes the Company's current environment, the procurement process from defining the technical requirements, through the various tender rounds to the final selection of the EDR solution. Subsequently, the thesis describes the actual process of deploying the selected EDR solution in the Company's environment.

Another objective of this thesis is to compare the actual selection and deployment in the Company's environment with best practices.

Keywords: EDR, XDR, antivirus, corporate environment, cybersecurity, malware, defence in-depth, layered security, best practice, selection procedure

Obsah

1 Úvod

Kybernetická bezpečnost je obsáhlý a neustále se vyvíjející odvětví informačních technologií, které se zabývá ochranou počítačových systémů, sítí a dat před neoprávněným přístupem, zneužitím nebo poškozením. Podobně jako informační technologie se dělí na několik oblastí, například ochrana hardware a software, správa identit, reakce na incidenty, vzdělávání zaměstnanců, monitorování a audit nebo právní a regulatorní aspekty. O těchto a dalších aspektech v kybernetické bezpečnosti bylo napsáno mnoho odborných knih a článků, minimum se jich však věnuje výběru a nasazení specifických řešení. Nedostatek pozornosti věnovaný této problematice a zároveň osobní zkušenost s výběrem a nasazením EDR řešení ve společnosti s 6000 zaměstnanci dala podnět k napsání této bakalářské práce.

Na začátku této práce je definován její cíl a použitá metodika. Teoretická část se zaměřuje na současnou situaci v kybernetické bezpečnosti, hrozby, kterým firmy čelí, popis EDR, porovnání s ostatními bezpečnostními produkty, jak tyto produkty mohou pomoci firmám bránit se nejčastějším kybernetickým útokům, jaký je doporučený postup při výběru a nasazení takového produktu.

Praktická část se následně zabývá popsáním průběhu výběrového řízení od definování požadavků, přes výběr kandidátů a průběh Proof of Concept (PoC) testování až po výsledné nasazení vybraného řešení do produkčního prostředí Společnosti s několika dceřinými společnostmi a více než 6000 zaměstnanci.

Bakalářská práce používá neutrální označení Společnost, Uchazeč* a během popisu implementace je vybraný Uchazeč označován jako Dodavatel, jelikož autor podepsal se Společností Smlouvu o mlčenlivosti a je oprávněn sdělit pouze obecné informace, které nevystaví danou Společnost potencionálnímu kybernetickému útoku. Veškerá vyobrazení obrazovek a nastavení jednotlivých produktů mají pouze informativní charakter a v žádném případě nezobrazují prostředí Společnosti.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je popsání současné situace v kyberbezpečnosti a hrozbách, kterým firmy čelí, jak je možné se proti těmto hrozbám bránit pomocí antivirových, EDR a XDR řešení, porovnání těchto řešení a popsání best practice pro výběr tohoto řešení. V praktické části popsání reálného výběru a nasazení EDR řešení v korporátním prostředí a porovnání s best practice.

2.2 Metodika

V rámci BP bude v teoretické části popsáno, co je to EDR, rozdíly mezi klasickými antiviry, EDR a XDR. Jednotlivé výhody a nevýhody, jaké jsou současné bezpečnostní hrozby a jak tyto nástroje mohou firmám pomoci se jim bránit. Dále bude popsáno, jaké jsou best practice pro nasazení EDR a jejich místo v in-depth security a layered security. V praktické části budou řešeny samotné požadavky pro výběrové řízení, předvýběr kandidátů, POC, výběr a samotné nasazení ve zvolené společnosti a porovnání reálného nasazení s best practice.

Informace budou čerpány z odborných knih a článků, stránek výrobců softwaru, konzultačních společností, internetových médií věnujících se informačním technologiím a kybernetické bezpečnosti. Informace ohledně výběrového řízení budou čerpány z interního dokumentu Společnosti.

3 Teoretická východiska

3.1 Současná situace v kybernetické bezpečnosti

Kybernetická bezpečnost je kritická a dynamická oblast, která se dotýká všech aspektů našeho života a průmyslových odvětví. Současný stav kybernetické bezpečnosti se vyznačuje několika výzvami a příležitostmi, které vyžadují neustálou ostražitost a spolupráci všech zúčastněných stran.

Podle Huntleyho (2023) jednou z těchto výzev bylo napadení Ukrajiny Ruskou federací v únoru roku 2022, kterému předcházely kybernetické útoky na kritickou infrastrukturu státu a ukrajinské společnosti. Kybernetické útoky na firmy a infrastrukturu probíhají neustále, avšak v roce 2022 se zvýšil počet kybernetických útoků na společnosti a uživatele v zemích NATO o více než 300 % oproti roku 2020. Za tímto nárůstem stojí podpora Ukrajiny západními zeměmi, ale také sankce uvaleny Evropskou unií nebo Spojenými státy. Na doporučení bezpečnostních složek (NÚKIB, 2022) došlo k omezení nebo úplnému odstranění softwaru vyvinutého ruskými společnostmi ve firemním a státním prostředí, například bezpečnostní produkt od firmy Kaspersky nebo Any.Run, interaktivní online sandbox pro testování podezřelých odkazů a souborů (Amante, 2022).

Pipikate a ostatní spoluautoři (2021) tvrdí, že rostoucí složitost a sofistikovanost kybernetických útoků, zejména útoků zaměřených na kritickou infrastrukturu, dodavatelské řetězce, zdravotnické systémy a volby, je další výzvou, které musí organizace čelit. Tyto útoky využívají zranitelnosti softwaru, hardwaru, cloudových služeb a lidského faktoru a mohou mít ničivé důsledky pro národní bezpečnost, veřejnou bezpečnost a ekonomickou stabilitu. Aby mohly organizace těmto útokům čelit, musí přijmout strategii hloubkové obrany, která zahrnuje více vrstev ochrany, detekce a reakce. Musí také investovat do zpravodajství a analýzy hrozeb a sdílet informace a osvědčené postupy s ostatními organizacemi a vládními agenturami.

Společnost McKinsey & Company (2022) vnímá jako další výzvu pro organizace rychlé zavádění nových technologií, jako je umělá inteligence, strojové učení, 5G a kvantová výpočetní technika, které přinášejí obrovské výhody, ale také nová rizika a etická dilemata. Tyto technologie mohou umožnit nové formy kybernetických útoků, jako jsou například deepfakes nebo phishingové emaily, které jsou jazykově i gramaticky správně (Caufield, 2023), nepřátelské strojové učení nebo kvantový hacking, a vytvářet nová zranitelná místa v oblasti soukromí, bezpečnosti a správy. Aby organizace mohly tyto technologie používat

bezpečně a zodpovědně, musí přijmout přístup založený na rizicích, který zohledňuje potenciální dopad a pravděpodobnost kybernetických hrozeb. Také musí již od prvního návrhu zavést zásady zabezpečení, které zabudují bezpečnost do každé fáze procesu vývoje a nasazení. V neposlední řadě musí podporovat kulturu etiky a odpovědnosti, která zajistí vhodné používání těchto technologií a dohled nad nimi (McKinsey & Company, 2022).

Velkým problémem pro firmy všech velikostí je rostoucí nedostatek kybernetických dovedností a talentů, který omezuje schopnost organizací bránit se kybernetickým hrozbám a reagovat na incidenty. Podle zprávy ISACA 2023 State of Cybersecurity má 62 % organizací neobsazené pozice v oblasti kybernetické bezpečnosti a 70 % uvádí, že jejich týmy kybernetické bezpečnosti nemají dostatek zaměstnanců (Lau, 2023). Zpráva také zdůrazňuje potřebu větší rozmanitosti a začlenění pracovníků v oblasti kybernetické bezpečnosti, stejně jako více možností školení a certifikace. Aby organizace tento problém vyřešily, musí přijmout strategii řízení talentů, která zahrnuje získávání, udržení, rozvoj a posílení postavení odborníků na kybernetickou bezpečnost. Musí také využívat alternativní zdroje talentů, jako je outsourcing, automatizace nebo crowdsourcing (Lau, 2023). Kromě toho musí podporovat vzdělávání a povědomí o kybernetické bezpečnosti na všech úrovních a ve všech funkcích organizace (Pipikate, et al., 2021).

Důležité je také vyvíjející se regulační prostředí a požadavky na dodržování předpisů, jejichž cílem je zlepšit standardy a postupy kybernetické bezpečnosti napříč odvětvími a geografickými oblastmi. Tyto předpisy však představují výzvu i pro organizace, které působí ve více jurisdikcích nebo mají složité dodavatelské řetězce. (Pipikate, et al., 2021) Například obecné nařízení Evropské unie o ochraně osobních údajů (GDPR) ukládá přísná pravidla ochrany údajů a soukromí, zatímco americká certifikace CMMC (Cybersecurity Maturity Model Certification) vyžaduje, aby dodavatelé v oblasti obrany splňovali určitou úroveň kybernetické bezpečnosti. (McKinsey & Company, 2022) Od roku 2023 také vstupuje v platnost aktualizované nařízení Network and Information Security verze dvě neboli NIS2. Toto nařízení nahrazuje původní NIS z roku 2016, rozšiřuje oblast působnosti a mění zařazení firem do dvou kategorií essential (s vyšším zájmem) a important (s nižším zájmem). Organizace v obou kategoriích musí zavést technická, provozní a organizační opatření, aby zvládly rizika ohrožující bezpečnost jejich sítí a informačních systémů a aby zabránily incidentům nebo minimalizovaly jejich dopad. Hlavní rozdíl mezi nimi však spočívá v tom, že subjekty s nižším zájmem budou čelit nižším finančním sankcím a budou podléhat reaktivnímu dohledu ze strany orgánů na rozdíl od proaktivního dohledu

vyhrazeného pro subjekty s vyšším zájmem. (European Commision, 2023) Aby organizace vyhověly těmto předpisům, musí přijmout rámec řízení, který sladí jejich zásady a postupy kybernetické bezpečnosti s příslušnými zákony a normami. Musí také zavést účinné kontrolní mechanismy a audity, které prokazují jejich stav a výkonnost v oblasti dodržování předpisů. Kromě toho musí spolupracovat s regulačními orgány a tvůrci politik, aby jim poskytly zpětnou vazbu a pokyny k vývoji a provádění těchto předpisů. (Tiel, 2023)

3.2 Nejčastější hrozby, kterým firmy čelí

V roce 2023 čelí organizace několika významným hrozbám v oblasti kybernetické bezpečnosti. Tyto hrozby se neustále vyvíjejí a společnosti musí zůstat ostražité a proaktivní, aby ochránily své systémy a data. Tato práce se zaměří na nejčastější kybernetické bezpečnostní hrozby, kterým organizace čelí v současnosti. (BDO Digital, 2022)

3.2.1 Malware

Malicious (škodlivý) software zkráceně malware je software, jehož autor má škodlivé úmysly. Tvůrci škodlivého softwaru se snaží narušit důvěrnost, integritu a/nebo dostupnost dat a/nebo systémů, které je zpracovávají, přenášejí a ukládají. Většina rodin malwaru dnes představuje smíšené hrozby. Před mnoha lety byly hrozby oddělené – byly to buď červi, nebo zadní vrátka, ale ne obojí. Dnes má většina malwaru vlastnosti více kategorií malwaru. Analytici v antimalwarových laboratořích, kteří zpětně analyzují vzorky malwaru, obvykle klasifikují malware podle primárního nebo nejvýraznějšího způsobu chování každého vzorku. Například malware může vykazovat vlastnosti červa, trojského koně a ransomware. Analytik jej může klasifikovat jako ransomware, protože je to jeho dominantní chování nebo vlastnost (Rains, 2020).

Níže jsou popsány příklady druhů škodlivého softwaru:

Trojské koně jsou nejrozšířenější kategorií škodlivého softwaru posledních deset nebo více let. Trojský kůň je program nebo soubor, který se prezentuje jako jedna věc, i když je ve skutečnosti něčím jiným, stejně jako příběh o trojském koni, na kterém je založen. Uživatel je oklamán, aby si jej stáhl a otevřel nebo spustil. Trojské koně se nešíří pomocí neopravených zranitelností nebo slabých hesel jako červi; ale spoléhají se na sociální inženýrství. Jednou variantou je trojský kůň s backdoorem. Jakmile je uživatel přiměn ke spuštění škodlivého programu (škodlivé mohou být i skripty a makra v kancelářských dokumentech), trojský kůň s backdoorem poskytuje útočníkům vzdálený přístup

k infikovanému systému. Jakmile získají vzdálený přístup, mohou potenciálně krást identity a data, krást softwarové a herní klíče, instalovat software a další škodlivý software podle vlastního výběru, přidávat infikovaný systém do botnetů a provádět tzv. projekty pro útočníky atd. Projekt může zahrnovat vydírání, útoky typu DDoS (Distributed Denial of Service), ukládání a distribuci nelegálního a pochybného obsahu nebo cokoli jiného, za co jsou útočníci ochotni vyměnit nebo prodat přístup do své sítě napadených systémů. Další variantou jsou trojské stahovače a droppery. Jakmile je uživatel oklamán a spustí škodlivý program, trojský kůň sám od sebe rozbalí další škodlivý software nebo stáhne další škodlivý software ze vzdálených serverů. Výsledkem je obvykle stejná škodlivá služba, která ze systému vytěží všechna důležitá data. Trojské stahovače a droppery byly mezi útočníky v letech 2006 a 2007 v módě, ale od té doby se dramaticky objevují v omezených časových úsecích. Jedním příkladem trojského downloaderu a dropperu je nechvalně známá hrozba Zlob. Uživatelé ji podvodně instalovali do svých systémů, když navštívili škodlivé webové stránky, které obsahovaly video, jež chtěli sledovat. Po kliknutí na požadované video jim webová stránka oznámila, že nemají nainstalovaný správný video kodek pro sledování videa. Webová stránka rovnou nabídla stažení video kodeku, aby uživatel mohl video zobrazit. Pokud si uživatel skutečně stáhl a nainstaloval Zlob, byl vystaven vyskakovacím reklamám na bezplatný "bezpečnostní software", který měl pomoci zabezpečit jeho systém. Uživatelé, kteří klikali na reklamy, stahovali a instalovali bezpečnostní software, poskytovali útočníkům stále větší kontrolu nad svými systémy (Rains, 2020).

Exploity jsou škodlivé kódy, které využívají zranitelnosti umožňující útočníkovi ohrozit důvěrnost, integritu nebo dostupnost hardwaru nebo softwaru. Ne všechny zranitelnosti jsou stejné; některé zranitelnosti mají v případě zneužití větší potenciální dopad na systém než jiné. Zneužití kritických zranitelností jsou útočníky velmi vyhledávaná, poskytují jim totiž nejlepší šanci převzít plnou kontrolu nad zranitelným systémem a spustit libovolný kód podle vlastního výběru. Tento kód může dělat cokoli, co může dělat uživatelský účet, pod kterým je spuštěn. Může například stahovat další škodlivý software ze serverů na internetu, což útočníkům umožní vzdáleně ovládat systém, krást identity a data, přidat systém do botnetu atd. Zpracované exploity na zranitelnosti webových prohlížečů, operačních systémů a prohlížečů souborů (pro formáty souborů jako .pdf, .doc, .xlsx atd.) mohou mít vzhledem k všudypřítomnosti těchto produktů velkou cenu. V důsledku toho se v posledních dvou desetiletích vyvinul sofistikovaný trh s nabídkou a poptávkou po exploitech. Exploity jsou nejčastěji doručeny pomocí phishingu, kterému se podrobněji

věnuje jedna z dalších kapitol. Útočník může například doručit exploit vytvořením škodlivého souboru .pdf nebo .docm, který je navržen tak, aby zneužil konkrétní neopravenou zranitelnost v prohlížeči, jako je Adobe Acrobat Reader nebo Microsoft Word. Pokud oběť otevře soubor pomocí programu, který není opraven na zranitelnost, kterou útočník používá, a pokud nejsou zavedena žádná jiná opatření na její omezení, je zranitelnost v systému zneužita a může dojít ke spuštění libovolného kódu podle útočníkova výběru. Odesílatel, v tomto případě, útočník, se může vydávat za spolupracovníka nebo přítele oběti. Protože oběť svému spolupracovníkovi nebo příteli důvěřuje, otevře přílohu e-mailu a exploit se spustí. Exploity také mohou být umístěny na webových stránkách jako soubory ke stažení pro oběti, zasílány prostřednictvím sociálních sítí nebo distribuovány na USB discích a jiných vyměnitelných médiích. Sada exploitů je knihovna exploitů s určitým softwarem pro správu, který útočníkům usnadňuje řízení útoků využívajících exploity. Tyto sady mohou obsahovat libovolný počet exploitů pro libovolný počet produktů. Sada exploitů může útočníkům poskytnout také webové stránky, které usnadňují distribuci exploitů obětem. Některé druhy softwaru pro správu zabudované do sady exploitů pomáhají útočníkům pochopit, které exploity úspěšně využívají zranitelnosti v systémech obětí a které ne. To útočníkům pomáhá lépe se rozhodovat, které exploity použít a kde maximalizovat návratnost svých investic. Tento software pro správu může útočníkům také pomoci identifikovat a nahradit exploity na jejich stránkách, které již nejsou účinné, novými exploity. Mezi příklady sad exploitů patří Angler (známý také jako Axpergle), Neutrino a nechvalně známá sada exploitů Blackhole (Rains, 2020). Tento přístup podporuje obchodní model a vedl k vytvoření nového termínu Malware as a Service (MaaS) (CrowdStrike, 2022).

Počítačový virus je typ škodlivého softwaru, který se šíří mezi počítači a způsobuje poškození dat a softwaru. Je navržen tak, aby narušil systémy, způsobil velké provozní problémy a vedl ke ztrátě a úniku dat. Viry se obvykle připojují ke spustitelnému hostitelskému souboru, což způsobí, že se jejich virový kód spustí při otevření souboru (Stephenson, 2020). Kód se pak bez souhlasu uživatele šíří z dokumentu nebo softwaru, ke kterému je připojen, prostřednictvím sítí, disků, programů pro sdílení souborů nebo infikovaných e-mailových příloh. Počítačový virus může zůstat neaktivní, dokud není spuštěn otevřením infikovaného souboru nebo programu. Protože infikují soubory a/nebo Master Boot Record (MBR) systémů, někdy nevybíravě, mohou být velmi "hlučnou" hrozbou, kterou lze snadno odhalit, ale obtížně zneškodnit (Rains, 2020). Některé viry jsou navrženy tak, aby kradly nebo poškozovaly data, zatímco jiné jsou vytvořeny tak, aby

destabilizovaly program nebo systém a potenciálně jej učinily nepoužitelným. Jiné jsou jednoduše vytvořeny programátorem pro zábavu a mohou jednoduše zobrazit obrázek nebo textovou zprávu při zapnutí počítače nebo otevření aplikace (Torres, 2017).

Zdá se, že v posledním desetiletí se viry u některých útočníků vrátily do módy. Dnešní tvůrci virů obvykle neinfikují pouze soubory jako jejich předchůdci před desetiletími, ale mohou být nápaditější a zákeřnější. Je známo, že moderní viry po infikování systému stahují další škodlivý software, deaktivují antimalwarový software, kradou přihlašovací údaje uložené v mezipaměti, zapínají mikrofon a/nebo videokameru počítače, shromažďují audio a video data, otevírají útočníkům zadní vrátka a odesílají ukradená data na vzdálené servery, kde si je útočníci mohou vyzvednout (Stephenson, 2020). V moderní době nejsou viry zdaleka tak rozšířené jako trojské koně nebo potenciálně nežádoucí software, ale zdá se, že vždy existuje určitá úroveň detekce (Rains, 2020).

3.2.2 **Ransomware**

Ransomware je typ škodlivého softwaru, který zašifruje data oběti nebo zablokuje její zařízení a za obnovení přístupu požaduje výkupné. Platba výkupného je nejčastěji požadována formou kryptoměn (IBM, 2023a). Prvního listopadu 2023 podepsala Česká republika spolu dalšími 50 státy, kteří jsou členy International Counter Ransomware Initiative, prohlášení, ve kterém se mimo jiné zavázala, že státní instituce nebudou platit případné výkupné v případě napadaní ransomware. (The White House, 2023) Doporučení neplatit vydal i Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) pro firmy, aby nedocházelo k povzbuzení útočníků k dalším útoků. (NUKIB, 2023) Dalším důvodem je, že neexistuje žádná záruka obnovení dat. K infikování počítače nebo sítě obvykle využívá bezpečnostních zranitelností, často prostřednictvím phishingových útoků nebo škodlivých webových stránek (Baker, 2023).

Ransomware se dělí na tři hlavní typy. Šifrovací ransomware nebo kryptografický ransomware, tento typ šifruje data oběti a útočník poté požaduje výkupné výměnou za dešifrovací klíč. Nešifrující neboli ransomware blokující obrazovku, tento typ uzamkne celé zařízení oběti, obvykle tím, že zablokuje přístup k operačnímu systému. Zastrašující ransomware, zobrazuje uživateli vyskakovací okna s oznámením, že jejich systém je infikován virem a odkazuje je na falešný, škodlivý, software, který má viry odstranit (Baker, 2023).

Obrázek 1 Obrazovka s požadavkem na výkupné, WannaCrypt/WannaCry ransomware

Zdroj: (Microsoft Defender Security Research Team, 2017)

Útoky ransomware se neustále vyvíjejí a poslední dobou zahrnují útoky s dvojím a trojím vydíráním (IBM, 2023a). Při dvojitém vyděračském útoku útočník nejen zašifruje data oběti, ale také vyhrožuje jejich zveřejněním na internetu. Trojitý vyděračský útok jde ještě o krok dále a hrozí, že ukradená data použije k útoku na zákazníky nebo obchodní partnery oběti (Baker, 2023).

Ransomware je obvykle doručován jedním z následujících způsobů. Phishingové e-maily jsou nejběžnější způsob doručení (Baker, 2023). Útočníci používají legitimně vypadající e-maily, aby oběti přiměli kliknout na škodlivou adresu URL nebo otevřít přílohu obsahující malware. Přes protokol vzdálené plochy (RDP). RDP je komunikační protokol, který umožňuje správcům IT přistupovat k systémům. Pokud je odhalen, může se stát vstupní branou pro útoky ransomware. Warezové stránky, torrenty a cracknuté aplikace jsou jedním z nejčastějších míst, kde se lze nakazit ransomware. K nákaze ransomware může vést také pouhá návštěva webové stránky nebo kliknutí na reklamu, která obsahuje škodlivý software (IBM, 2023a).

3.2.3 Phishing

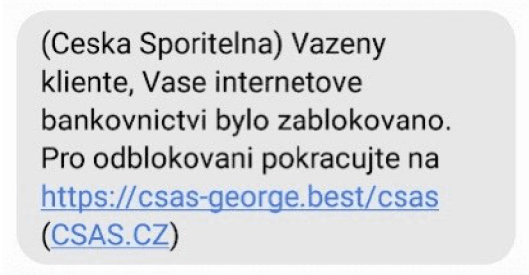
Phishing je typ kybernetického útoku, který se provádí především prostřednictvím e-mailu, ale může být proveden i prostřednictvím textové zprávy, označovaný jako smishing

neboli SMS Phishing, telefonního hovoru označovaný jako vishing neboli voice phishing. Cílem phishingu je vylákat od obětí jejich osobní a finanční údaje. Při phishingových útocích se útočník často vydává za důvěryhodný subjekt, například banku nebo oblíbenou webovou stránku, aby získal důvěru oběti. Útočník obvykle zašle e-mail nebo textovou zprávu, která se tváří jako zpráva od důvěryhodného subjektu, a požádá oběť o poskytnutí citlivých informací, jako jsou uživatelská jména, hesla, čísla kreditních karet nebo rodná čísla (Lenaerts-Bergmans, 2022). V některých případech může útočník připojit také odkaz na podvrženou webovou stránku, která vypadá stejně jako legitimní webová stránka, aby oběť dále oklamal a přiměl ji k zadání údajů (Ozkaya & Diogenes, 2019).

Spear phishing je cílenější forma phishingu. Namísto hromadného rozesílání e-mailů velkému počtu lidí jsou útoky typu spear phishing zaměřeny na konkrétní osoby nebo společnosti. Tyto útoky vyžadují od útočníka značnou míru pátrání, aby shromáždil dostatek informací o cíli a útok vypadal důvěryhodně (Lenaerts-Bergmans, 2022). Tyto informace mohou zahrnovat jméno cíle, e-mailovou adresu, pracovní pozici a konkrétní podrobnosti o jeho pracovním nebo osobním životě. Cíl spear phishingu je stejný jako u běžného phishingu: přimět cíl k odhalení citlivých informací nebo k instalaci malwaru do jeho zařízení (Ozkaya & Diogenes, 2019).

Phishingové emaily a podvodné zprávy obecně mají zpravidla několik společných rysů. Často přicházejí z e-mailových adres, které vypadají podobně jako legitimní, ale mají drobné rozdíly, například info@skooda-auto.cz, kdy doména obsahuje nějaké písmeno navíc nebo je naopak postrádá, či má jinou doménu, jak je vidět na Obrázku 2.

Obrázek 2 Podvodná SMS vydávající se za Českou spořitelnu, doména .best místo .cz



Zdroj: (Česká spořitelna, 2019)

Mnoho phishingových e-mailů je špatně napsaných a obsahují pravopisné a gramatické chyby. Toto se však poslední dobou mění díky nasazení technologií jako je například ChatGPT. (Caufield, 2023) Často se snaží vyvolat pocit naléhavosti nebo strachu, aby oběť

přiměly k bezmyšlenkovitému jednání. Například pokud nezareaguje dostatečně rychle, přijde o všechny peníze na bankovním účtu. Phishingové e-maily často obsahují odkazy na falešné webové stránky nebo přílohy obsahující škodlivý software. Zprávy žádají o poskytnutí osobních údajů nebo údajů k platebním kartám. Velmi často využívají aktuální situace nebo ročního období, například žádost o příspěvek od vlády nebo zpráva od dopravce ohledně doručení balíku v době před Vánoci (Lenaerts-Bergmans, 2022).

3.2.4 **Supply chain attack**

Supply chain attack neboli útok na dodavatelský řetězec je typ kybernetického útoku, který se zaměřuje na méně bezpečné prvky dodavatelského řetězce (Haas, 2022). Jedná se o velmi účinný způsob prolomení zabezpečení vložením škodlivých knihoven nebo komponent do produktu bez vědomí vývojáře, výrobce nebo koncového uživatele. Cílem je odcizit citlivá data, získat přístup do vysoce citlivých prostředí nebo získat vzdálenou kontrolu nad konkrétními systémy (Lenaerts-Bergmans, 2023).

Útoky na dodavatelský řetězec lze provádět jak na software, tak na hardware. Softwarové útoky dodavatelského řetězce vnášejí do aplikace škodlivý kód s cílem infikovat všechny uživatele aplikace, zatímco hardwarové útoky dodavatelského řetězce kompromitují fyzické komponenty za stejným účelem (Haas, 2022).

Historicky se útoky na dodavatelský řetězec týkaly útoků na důvěryhodné vztahy, kdy byl napaden nezabezpečený dodavatel v řetězci, aby byl získán přístup k jeho větším obchodním partnerům. Dnes však větší obavy vzbuzuje útok na softwarový dodavatelský řetězec. Softwarové dodavatelské řetězce jsou obzvláště zranitelné, protože dnešní software není psán od nuly, ale obsahuje mnoho hotových komponent, jako jsou rozhraní API třetích stran, otevřený zdrojový kód a proprietární kód dodavatelů softwaru. Průměrný softwarový projekt má dnes 203 závislostí. Pokud populární aplikace obsahuje kompromitovanou závislost, je kompromitována každá společnost, která si od tohoto dodavatele stáhne software, takže počet obětí může exponenciálně růst (Lenaerts-Bergmans, 2023).

Počet útoků na dodavatelský řetězec vzrostl o 430 %, protože s tím, jak se organizace zlepšily v oblasti zabezpečení svých prostředí, se útočníci zaměřili na lehčí cíle a našli kreativnější způsoby, jak znesnadnit odhalení svého úsilí a zvýšit pravděpodobnost, že dosáhnou požadovaných cílů (Lenaerts-Bergmans, 2023).

Jedním z nejznámějších příkladů útoku na dodavatelský řetězec je zranitelnost Log4j, známá také jako Log4Shell. Zranitelnost Log4j byla odhalena 10. prosince 2021. Jedná

se o kritickou zranitelnost v logovacím frameworku Log4j od společnosti Apache, která umožňuje útočníkům vzdáleně spustit kód v jakémkoli zranitelném prostředí (Check Point Research Team, 2021). Tato zranitelnost má hodnocení CVSS 10, což je nejvyšší možné hodnocení. Protokol Log4j je široce používán a zabudován v každém produktu nebo webové službě založené na technologii Java, což velmi ztěžuje jeho ruční nápravu. Množství kombinací, jak ji lze zneužít, dává útočníkovi mnoho alternativ, jak obejít nově implementované ochrany. Tato zranitelnost byla zneužita při útoku na dodavatelský řetězec, protože Log4j je softwarový prvek používaný v široce distribuovaném softwaru. Taková narušení se velmi obtížně odhalují, a proto zůstávají dlouho neodhalena. Mnoho společností si navíc není vědomo, že byly napadeny. Zranitelnost Log4j měla významný dopad na bezpečnost dodavatelského řetězce a bylo obtížné ji opravit. Jde o nejhorší možný scénář, pokud jde o riziko dodavatelského řetězce (Haas, 2022). Index X-Force Threat Intelligence společnosti IBM zaznamenal mezi lety 2020 a 2021 34% nárůst počtu zneužití zranitelností, a to zejména kvůli Log4Shell (IBM, 2023b).

3.2.5 **Zero day útoky**

Zero day útok nebo také zranitelnost nultého dne je zranitelnost, která je zveřejněna předtím, než výrobce software vydal bezpečnostní aktualizaci, která ji opravuje. Tyto zranitelnosti jsou ze všech zranitelností nejcennější, protože útočníci a vlády jsou za ně ochotni zaplatit poměrně vysoké částky (za funkční exploit může jít o milion dolarů a více) (Fortinet, 2024).

Dokud není zranitelnost zmírněna, mohou ji hackeři zneužít k negativnímu ovlivnění počítačových programů, dat, dalších počítačů nebo sítě. Zero-day zranitelnosti nemají žádnou známou záplatu a uživatelské systémy nemají žádnou ochranu, takže je velmi pravděpodobné, že útoky budou úspěšné. Zneužití zero-day je taktika nebo metodika, kterou aktéři hrozeb používají k útokům na systémy s neznámými zranitelnostmi (Rains, 2020). Například zero-day malware je škodlivý program navržený útočníky tak, aby zneužíval těchto zranitelností. (Mishra, 2022)

Scénářem, kterého se týmy pro správu zranitelností obávají, je situace, kdy byla veřejně odhalena kriticky hodnocená zranitelnost nultého dne v softwaru nebo hardwaru, který mají ve svém prostředí. To znamená, že riziko zneužití může být velmi vysoké a že aktualizace zabezpečení, která by mohla zneužití zranitelnosti zabránit, není veřejně dostupná. (Mishra, 2022) Někdy v těchto scénářích existují „workarounds“, které lze

implementovat, aby se ztížilo nebo znemožnilo zneužití zranitelnosti. Tato řešení, jako jsou například speciální konfigurace systému, které zabrání zneužití, jsou obvykle zamýšlena jako dočasná, než je vydána opravná aktualizace (Rains, 2020). Často změna konfiguračního nastavení jako řešení problému také znemožní funkce, které byly předtím k dispozici. Jediný způsob, jak zranitelnost vyřešit s nejvyšší mírou jistoty a nejmenším dopadem, je nainstalovat aktualizaci, která zranitelnost opravuje (Fortinet, 2024).

Ještě horším scénářem je situace, kdy výrobce vydá aktualizaci zabezpečení pro zneužitelnou kritickou zranitelnost, ale aktualizace zranitelnost zcela neopraví. V tomto scénáři je existence zranitelnosti veřejně známá a veřejně dostupná aktualizace zabezpečení, která není stoprocentně účinná, v podstatě nakreslí mapu zranitelnosti, kterou mohou útočníci využít. Typicky se v takových scénářích kód pro zneužití takové zranitelnosti velmi rychle stane veřejně dostupným a široce rozšířeným na internetu. Tento scénář může znít teoreticky, ale bohužel se za posledních dvacet let několikrát stal. Nejnovějším a nejlepším příkladem zero day útoku je výše zmíněná zranitelnost "Log4j" (Mishra, 2022).

Časovou osu zneužití zranitelnosti v režimu nultého dne rozdělili bezpečnostní výzkumníci do sedmi samostatných fází (Mishra, 2022):

1. Zranitelnost je vytvořena: Vývojář vydá software, který nevědomky obsahuje zranitelný kód.
2. Zneužití je zveřejněno: Zranitelnost objeví záškodník dříve, než se o ní vývojář dozví, nebo než ji vývojář stihne opravit či vydat aktualizaci. Hacker pak napíše a nasadí exploit, dokud je zranitelnost stále otevřená.
3. Zranitelnost je objevena: Výrobce se o zranitelnosti dozví, ale nemá k dispozici opravu.
4. Odhalení zranitelnosti: Výrobce a/nebo bezpečnostní výzkumníci zranitelnost veřejně oznámí a upozorní tak uživatele a útočníky na její existenci.
5. Uvolnění antivirových signatur: Pokud útočníci vytvořili malware nultého dne, který se na zranitelnost zaměřuje, mohou dodavatelé antivirových programů rychle identifikovat jeho signaturu a poskytnout proti němu ochranu. Systémy však mohou zůstat zranitelné, pokud existují jiné způsoby, jak zranitelnost zneužít.
6. Vydání bezpečnostní záplaty: Výrobce zveřejní opravu zranitelnosti.

Útok je buď úspěšný, což pravděpodobně vede k odcizení identity nebo informací útočníkem, nebo dodavatel vytvoří opravu, která omezí šíření zranitelnosti. Jakmile

je záplata napsána a použita, zranitelnost již není považována za zero-day zranitelnost (Fortinet, 2024).

3.2.6 Útoky na cloudové technologie

Útoky na cloudové technologie jsou i nadále výrazným a znepokojivým trendem, který se zaměřuje na zranitelná místa v cloudových technologiích a infrastruktuře. Cílem těchto útoků je kompromitovat citlivá data organizace, narušit její provoz nebo získat neoprávněný přístup. Cloudová prostředí jsou zranitelná vůči aktérům hrozeb, kteří se snaží využít slabé kontroly přístupu k průniku do cloudových úložišť. Velkou hrozbou pro moderní cloudy jsou také útoky typu DDoS (Distributed Denial-of-Service), které mohou zahltit cloudové servery a způsobit rozsáhlé narušení služeb. V roce 2023 došlo zejména k výraznému nárůstu krádeží informací v cloudu, kdy finančně motivované nástroje kradou data ze zranitelných nebo špatně nakonfigurovaných cloudových prostředí (SentinelOne, 2023).

Důvodem pro rychlý vývoj cloudových služeb je jejich bezkonkurenční flexibilita, dostupnost a kapacita. Odborníci na kybernetickou bezpečnost však varují, že cloud není bezpečný, a rostoucí počet útoků organizovaných v cloudu tato tvrzení potvrzuje. Cloud má jednu zásadní slabinu: vše je sdílené. Lidé a organizace musí sdílet úložiště, procesorová jádra a síťová rozhraní. Hackerům proto stačí překonat bezpečnostní opatření, která poskytovatelé cloudu zavedli, aby zabránili lidem ve vzájemném přístupu k datům. Protože dodavatel vlastní hardware, má způsoby, jak tato opatření obejít. S tím hackeři vždy počítají a snaží se proniknout na samotný backend cloudových služeb, kde se nacházejí všechna data. Existuje omezení, kolik toho mohou jednotlivé organizace udělat pro zajištění bezpečnosti dat, která ukládají v cloudu. Bezpečnostní prostředí cloudu je do značné míry určeno poskytovatelem. Zatímco jednotlivé organizace mohou být schopny zajistit neproniknutelné zabezpečení svých lokálních serverů, nemohou totéž rozšířit na cloud. Existují rizika, která vznikají, když se kybernetická bezpečnost stává odpovědností jiné strany. Dodavatel nemusí být při zabezpečení dat zákazníků například tak důsledný. Cloud také zahrnuje používání sdílených platforem s dalšími osobami, ale uživatel cloudu má omezené možnosti kontroly přístupu. Zabezpečení je z velké části ponecháno na poskytovateli (Ozkaya & Diogenes, 2019). Žádná organizace ani poskytovatel cloudových služeb však nedokáže eliminovat všechny bezpečnostní hrozby a zranitelnosti, takže vedoucí pracovníci firem musí zvážit výhody zavedení cloudu a míru rizika zabezpečení dat, kterou jsou ochotni akceptovat (Mishra, 2022).

Existuje mnoho dalších důvodů, proč se odborníci na kybernetickou bezpečnost obávají, že cloud není bezpečný (Ozkaya & Diogenes, 2019). V posledních letech se zvýšil počet útoků na poskytovatele cloudových služeb a společnosti využívající cloud. Jednou ze společností, která se stala obětí hackerských útoků na cloud, je Target, síť diskontních supermarketů ve Spojených státech amerických. Prostřednictvím phishingových e-mailů se útočníkům podařilo získat přihlašovací údaje ke cloudovým serverům společnosti. Po ověření totožnosti byli schopni ukrást údaje o kreditních kartách až 70 milionů zákazníků. Organizace byla údajně několikrát varována před možností takového útoku, ale tato varování byla přehlédnuta (Mishra, 2022).

3.3 Antivirus a EPP, EDR, XDR

V dynamické oblasti kybernetické bezpečnosti vyžaduje rostoucí sofistikovanost hrozeb stejně vyspělou a víceúrovňovou ochranu. Tradiční antivirová řešení, která kdysi tvořila základ zabezpečení koncových bodů, se vyvinula v komplexnější platformy ochrany koncových bodů (Endpoint Protection Platform, EPP), které nabízejí integrovanou sadu prostředků určených k odvrácení široké škály kybernetických hrozeb v bodě prvního kontaktu. V době, kdy jsou hrozby stále dokonalejší v obcházení prvotní obrany, se však důraz přesunul z prevence na rychlou detekci a účinnou reakci. Tento posun představují systémy detekce a reakce na koncových bodech ("Endpoint Detection and Response", EDR), které zajišťují nepřetržité monitorování, pokročilou detekci hrozeb a schopnosti reakce v reálném čase, čímž poskytují kritickou záchrannou síť v případě, že hrozby prolomí počáteční obranu. Složitost dnešních kybernetických hrozeb, které často cílí na více zranitelností současně, však vyžaduje ještě integrovanější přístup. Rozšířená detekce a reakce ("eXtended Detection and Response", XDR) představuje kulminaci tohoto vývoje strategie kybernetické bezpečnosti. Díky sjednocení více bezpečnostních produktů do uceleného, jednotného systému poskytuje XDR komplexní přehled, analýzu a reakci napříč sítěmi, koncovými body, cloudem a e-mailovými systémy, což představuje významný krok vpřed ve snaze překonat neustále se vyvíjející kybernetické hrozby (GEORGE, et al., 2021).

3.3.1 Antivirus a Endpoint Protection Platform (EPP)

První virus pojmenovaný Creeper byl vytvořen v roce 1971 Bobem Thomasem ze společnosti BBN Technologies jako Proof of Concept sebe replikujícího se kódu a jeho

hlavní funkcionalitou bylo zobrazení zprávy “I’m the creeper, catch me if you can!” neboli „Jsem Creeper, chyť mě, když to dokážeš!“ na obrazovkách napadených počítačů. Tento vir se šířil ARPANETem, sítí sdružující výzkumné organizace a předchůdce dnešního internetu. Přestože se nejednalo o škodlivý virus, bylo jasné, že je nutné vytvořit patřičná protiopatření. To vytvořil Ray Tomlinson, když vyvinul první antivirus s názvem Reaper, který na počítačích hledal a mazal vir Creeper (It, 2024).

V roce 1987 John McAfee vytvořil první komerční antivirový software poté, co jeho osobní počítač byl infikován „Brain“ virem a během oprav infikovaných počítačů se rozhodl zautomatizovat detekci a odstranění tohoto viru (Szor, 2005). Následovaly další společnosti, jako například ESET, Avast nebo Symantec, která vydala první antivirus na systém Macintosh (Sahay, 2024). Tyto první viry byly relativně jednoduché a často se šířily prostřednictvím infikovaných disket. Tehdejší antivirová řešení byla stejně primitivní a spoléhala se především na detekci založenou na signaturách. Tato metoda spočívala ve skenování systému na specifické řetězce kódu, které byly jedinečné pro známé viry. V roce 1990 bylo známo méně než 100 kmenů a výzkumníci počítačových virů mohli strávit týdny analýzou jediného viru díky tomu, že se počítačové viry šířily pomalu ve srovnání s rychlým šířením dnešních virů a malware (Szor, 2005).

S vývojem počítačových systémů a rozšířením internetu došlo pochopitelně i k vývoji a nárůstu škodlivého software a detekce založená na signaturách se ukázala jako nedostatečná, přestože je do dnešního dne v antivirovém software dostupná a k aktualizaci virových definic dochází minimálně jednou denně. Tyto virové definice obsahují hash nebo algoritmy nově objeveného škodlivého software, a tedy by se spíše hodilo je označovat jako malwarové definice, stejně jako antivirový software by měl být označený jako antimalwarový, přesto se nadále používá historicky zažité pojmenování (ESET, 2024b). S rozšířením malwaru, který je schopen měnit svůj kód, detekují dnešní antivirová řešení také chování jednotlivých spouštěných programů. Využívají k tomu například sandboxing, tedy spuštění programu nebo procesu v izolovaném prostředí nebo heuristickou analýzu, která porovnává chování programu s očekávaným chováním programu. Tyto technologie jsou označovány jako behaviorální detekce (Landesman, 2019). S rozvojem technologií jako je strojové učení, cloud a poslední dobou umělá inteligence, jsou tyto technologie implementovány i do antivirového softwaru (Info Exchange, 2022). Antivirový software, který má pouze lehkého klienta a veškeré informace se zpracovávají v cloudu je označovaný jako Next-Generation Antivirus (NGAV). Tato řešení mají výhodu v nižší zátěži koncového

zařízení a umožňují rychlejší detekci neustále se vyvíjejících hrozeb. Nejčastěji se lze setkat s řešeními, které kombinují všechny dostupné možnosti detekcí pro ochranu koncového zařízení bez citelného dopadu na výkon a také bez připojení k internetu (Aarness, 2023b).

Současná antivirová řešení často také obsahují další bezpečnostní funkcionality, a proto je možné se setkat s označením Endpoint Protection Platform. Mezi tyto funkcionality může mimo jiné patřit firewall, pro monitoring a správu síťové komunikace pomocí pravidel, Intrusion Prevention System (IPS), zabraňující síťovým hrozbám, Data Loss Prevention (DLP) pro blokování úniku citlivých informací nebo Device control (Správa zařízení) pro omezení připojených zařízená jako jsou například externí pevné disky nebo flashdisky a tím pádem omezit možnost nakažení malwarem nebo úniku informací (ESET, 2024c).

3.3.2 Endpoint Detection and Response

V roce 2013 pracovník společnosti Gartner Anton Chuvakin (Chuvakin, 2013) navrhl termín Endpoint Threat Detection and Response (ETDR), který se později zkrátil na Endpoint Detection and Response (EDR), pro systémy, které vznikly v důsledku omezení tradičních antivirových řešení. EDR řešení se zaměřují primárně na nepřetržité monitorování, detekci a reakci na kybernetické hrozby na úrovni endpointů a jsou navržena tak, aby organizacím poskytovala nástroje potřebné k identifikaci, prošetření a zmírnění hrozeb, které se vyhnuly tradičním bezpečnostním opatřením, jako je antivirový software. Základní funkcí EDR je sběr a analýza dat z koncových bodů s cílem odhalit podezřelou aktivitu, která je rovnou blokována nebo je bezpečnostním týmům poskytnuta možnost efektivně reagovat na incidenty (Aarness, 2023c).

Nepřetržitý sběr dat systémových procesů, síťového provozu, změn v registrech, aktivity souborů a událostí přihlášení probíhá pomocí agenta, který je nainstalovaný na koncovém zařízení, a následně jsou tato data odesílána do cloudu, kde probíhá jejich analýza. Některá řešení umožňují instalaci konzole pro správu i lokálně na servery společnosti kvůli ochraně dat, avšak toto řešení má jen omezené možnosti detekce (Aarness, 2023c). Sesbíraná data jsou analyzována v reálném čase pomocí strojového učení, umělé inteligence a technik jako je detekce anomálií, behaviorálních detekcí nebo i detekce signatur. Na základě výsledků této analýzy jsou vytvářeny indikátory kompromitace a následná upozornění pro bezpečnostní týmy. Reakce na tato upozornění mohou být do velké míry automatizovány například izolováním koncového zařízení od sítě, kdy jediná

povolená komunikace je management konzolí pro správu, aby bezpečnostní tým mohl daný incident prošetřit a vyhodnotit (BasuMallick, 2022). Avšak je za potřebí pokročilé nastavení a důsledné testování, aby byly limitovány reakce na false positive nálezy a tyto reakce neměly vliv na provoz koncových zařízení (Kayiş, 2019). Nejčastěji je reakce ponechána na bezpečnostním týmu, který vyhodnotí daný incident a na základě tohoto rozhodnutí může například přidat daný proces nebo soubor do výjimek, pokud se jedná o nepotvrzenou hrozbu nebo v případě potvrzené hrozby izolovat dané zařízení od sítě, odstranit škodlivý soubor či spustit předpřipravený skript pro odstranění malware (Trellix, 2024).

V přílohách 1 a 2 je možné porovnat dostupné informace u detekovaného malwaru u klasického antiviru a EDR.

Výhodou EDR řešení je shromažďování velkého množství dat a možnosti jejich zpětné analýzy, pokud se objeví nové indikátory kompromitace (Aarness, 2023c). Tato analýza probíhá automaticky za využití threat inteligence neboli informací o hrozbách, které jsou poskytovány jednak společnostmi vyvíjejících EDR řešení, tak externími společnostmi, například Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) projekt neziskové výzkumné skupiny spolupracující s vládou Spojených států (Trellix, 2024).

Společným cílem EDR a NGAV je pomáhat organizacím snižovat rizika předcházením kybernetickým útokům. Hlavním rozdíl je však v tom, kdy se používají a jak fungují. NGAV je preventivní složka zabezpečení koncových bodů, jejímž cílem je zabránit průniku kybernetických hrozeb do koncového zařízení. Ačkoli je NGAV důležitou první linií obrany podniku, není spolehlivá a žádné řešení, bez ohledu na to, jak je pokročilé, nemůže poskytnout stoprocentní ochranu. V případě, že hrozby obejdou antivirové řešení, EDR tuto aktivitu odhalí a umožní týmům zadržet protivníka dříve, než se může v síti pohybovat dále (Aarness, 2023a). Pokud je NGAV považován za první linií obrany, pak EDR je záchrannou sítí, která zachytí všechny hrozby, které proklouznou. Kromě detekce hrozeb shromažďuje EDR také údaje o útoku, včetně použitých Technik, Taktik a Postupů (TTP). To poskytuje bezpečnostnímu týmu důležité informace, včetně podrobností o aktérovi hrozby a dalších informací známých o útoku. Tato data pomáhají týmu rychle reagovat na hrozby a přesně se na ně zaměřit, aby se omezily škody (BasuMallick, 2022). Po odstranění hrozby je možné díky EDR řešení také shromáždit další podrobnosti o tom, jak k útoku došlo a jak se šířil, což může pomoci předcházet podobným útokům v budoucnu (CYNET, 2024).

3.3.3 Extended Detection and Response

Společnost Gartner definuje XDR jako jednotnou platformu pro detekci bezpečnostních incidentů a reakci na ně, která automaticky shromažďuje a koreluje data z různých proprietárních bezpečnostních komponent. (Firstbrook & Lawson, 2021) Jedná se o další vývoj Endpoint Detection and Response řešení, kdy tento systém shromažďuje a automaticky koreluje data z různých bezpečnostních vektorů, jako jsou e-maily, koncová zařízení, servery, cloudová prostředí a sítě, a umožňuje tak rychlejší detekci hrozeb a zlepšení efektivity vyšetřování a doby odezvy díky pokročilé bezpečnostní analýze (GEORGE, et al., 2021). Nástup XDR představuje významný vývoj v boji proti stále sofistikovanějším kybernetickým hrozbám, které se vyhýbají detekci tím, že využívají roztříštěnosti a nedostatečné propojenosti tradičních bezpečnostních řešení, čímž se postupem času zvyšuje efektivita těchto hrozeb (Aarness, 2023d). Bezpečnostní analytici, zahlcení záplavou výstrah z různých zdrojů, mají mezitím problém tyto hrozby efektivně třídit a prošetřovat, protože jsou limitováni omezenými a nesourodými možnostmi, které poskytují stávající bezpečnostní nástroje. XDR řeší tyto problémy agregací a korelací souborů dat napříč bezpečnostním spektrem, což umožňuje automatizovanou analýzu, která urychluje proces detekce (SentinelOne, 2024).

Kromě toho nedostatečná viditelnost mezi různými bezpečnostními řešeními dále komplikuje odhalování hrozeb a reakci na ně. Tradiční bezpečnostní produkty sice poskytují přehled o konkrétních aktivitách, ale často selhávají v integraci a korelaci dat napříč bezpečnostním prostředím, takže analytici mají roztříštěný pohled na potenciální hrozby (GEORGE, et al., 2021). Naproti tomu XDR poskytuje komplexní přístup k datovému uložišti, které zahrnuje detekce, telemetrii, metadata a síťové toky z jednotlivých bezpečnostních nástrojů. Tento konsolidovaný soubor dat obohacený o sofistikovanou analytiku a threat intelligence poskytuje analytikům ucelený kontext pro pohled na celý řetězec událostí zaměřený na útok, což výrazně zlepšuje možnosti detekce a vyšetřování (SentinelOne, 2024).

Proces vyšetřování, který je náročný kvůli obrovskému množství protokolů a výstrah bez jasných indikátorů, je díky XDR výrazně zefektivněn. Díky automatizaci vyšetřování hrozeb a eliminaci manuálních kroků poskytuje XDR analytikům bohatá data a analytické nástroje, které usnadňují detailní pochopení časové osy a cesty útoků napříč různými vektory. Tato schopnost je klíčová pro zavedení komplexní a účinné strategie reakce (SentinelOne, 2024).

Kromě zvýšení míry detekce hrozeb a doby reakce představuje XDR významný pokrok v metodikách detekce a reakce. Překračuje hranice EDR tím, že rozšiřuje ochranu mimo spravované koncové body na sítě, cloudová prostředí, servery, e-maily a další. Toto rozšíření umožňuje komplexnější přístup k detekci a reakci na hrozby, překonává omezení nástrojů pro analýzu síťového provozu a vylepšuje tradiční systémy správy bezpečnostních informací a událostí (SIEM) tím, že snižuje únavu z výstrah, zlepšuje korelaci bezpečnostních dat a zároveň umožňuje reagovat na zjištěné hrozby. (GEORGE, et al., 2021)

3.4 Porovnání schopností ochrany antivirem (NGAV), EDR a XDR proti nejčastějším hrozbám

V oblasti kybernetické bezpečnosti je důležité nasadit pokročilé obranné mechanismy k ochraně proti různým hrozbám, včetně malwaru, ransomware, útoků na dodavatelský řetězec a zero-day exploitů. Antivirový software, Endpoint Detection and Response (EDR) a Extended Detection and Response (XDR) jsou užitečné nástroje pro identifikaci, prevenci a zmírnění kybernetických hrozeb (GEORGE, et al., 2021).

Níže uvedená Tabulka 1 poskytuje souhrn toho, jak mohou antivirové technologie, EDR a XDR technologie nabídnout ochranu proti různým kybernetickým hrozbám, včetně malwaru, ransomware, phishingu, útoků na dodavatelský řetězec, zero-day útoků a cloudových útoků. Stojí za zmínku, že účinnost těchto bezpečnostních opatření se může lišit v závislosti na konkrétním implementovaném řešení a jeho konfiguraci. Proto je nezbytné, aby organizace pečlivě vyhodnotily své jedinečné bezpečnostní potřeby a efektivitu těchto technologií při ochraně svých digitálních aktiv.

Tabulka 1 Porovnání schopností ochrany antivirem (NGAV), EDR a XDR

HROZBA	ANTIVIR (NGAV)	EDR	XDR
Malware	Pomocí signatur a heuristiky	Monitorováním koncových zařízení na podezřelé aktivity	Monitorováním sítě, koncových zařízení a cloudu detekuje i sofistikovaný malware
Ransomware	Pomocí signatur a monitorování chování	Monitorováním změn souborů a podezřelého chování na koncových zařízeních	Monitorováním sítě, koncových zařízení a cloudu detekuje ransomware skrze celé prostředí
Phishing	Pomocí analýzy odkazů a příloh	Neochrání, detekuje až následný průnik útočníka nebo podezřelé chování na koncových zařízeních	Detekuje hrozby díky korelaci dat z emailů, koncových zařízení a sítě
Supply chain attack	Neochrání, pokud útočník nepoužil známý malware	Monitorováním aktivit skrze koncová zařízení a detekcí neobvyklého chování	Ještě lépe detekuje neobvyklé chování díky korelaci dat z celého prostředí
Zero day útok	Omezené možnosti, jelikož spoléhá na známé signatury	Analýzou aktivit na koncových zařízeních	Korelací dat z celého prostředí a využití pokročilé analytiky a strojového učení
Útok na cloudové prostředí	Částečná ochrana pomocí skenování souborů a aplikací	Monitorováním koncových zařízeních umístěných v cloudu	Korelací dat z cloudového prostředí a sítě

Zdroj: (Vlastní zpracování, 2024) (Yehushua & Kosayev, 2021) (Hand, 2023) (SentinelOne, 2024)

3.5 Best practice pro výběr a nasazení EDR

Websterův slovník (Merriam-Webster, 2024) definuje best practice jako postup, u kterého výzkum a zkušenosti prokázaly optimální výsledky a který je zaveden jako standard vhodný pro široké osvojení. Následováním best practice může společnostem uspořit nemalé finanční prostředky a pomoci jim vyhnout se potencionálním problémům (Mishra, 2022).

Výběr a implementace vhodného bezpečnostního řešení vyžaduje orientaci v množství produktů, z nichž každý má své jedinečné funkce a výhody (Mishra, 2022). Jedním ze základních aspektů, které zajistí, že zvolené řešení bude odpovídat firemním potřebám, je posouzení stávajících bezpečnostních nástrojů a politik, stejně jako identifikace konkrétních bezpečnostních problémů a rizik, jako jsou běžné vektory útoků a povaha citlivých dat. Dalším důležitým kritériem je počet zaměstnanců a koncových zařízení. Pro menší organizace může být proveditelná individuální správa zařízení, avšak s rostoucím počtem zaměstnanců a zařízení je zásadní zvolit řešení, které nabízí centralizované řízení pro zvýšení efektivity. Při řešení problémů s koncovými zařízeními na jednom místě může stačit lokální podpora, ale pro podniky, které využívají vzdálenou práci, je však zásadní zvolit řešení, které umožňuje vzdálený přístup k problémovým koncovým zařízením. Kromě toho je zásadní podpora roamingu a vzdálených zaměstnanců. V dnešní kultuře BYOD (Bring Your Own Device) je možnost vzdálené správy koncových zařízení nezbytná a bez robustního řešení zabezpečení může být správa zařízení, která se často připojují a odpojují od firemní sítě, náročná (Capterra, 2024).

Výběr vhodného řešení EDR vyžaduje důkladné prozkoumání spektra dostupných dodavatelů a softwaru s kritickým ohledem na funkce, které jsou v souladu s jedinečnými požadavky organizace (Capterra, 2024). Tento proces výběru zahrnuje zvážení schopností softwaru detekce hrozeb, schopností odezvy v reálném čase, škálovatelnosti, snadného nasazení a správy a schopnosti bezproblémové integrace se stávajícími bezpečnostními nástroji. Rozhodování mezi cloudovým a on premise nasazením závisí na faktorech, jako jsou náklady, rychlost poskytování služeb, možnosti vzdálené správy a kontrola organizace nad svými daty a také dostupnost funkcí, které nejsou ve velké většině při on premise nasazení dostupné. Dalším důležitým kritériem je správné načasování výběru, kdy je nutné začít včas, zejména před termínem obnovy stávajícího řešení, aby byl dostatek času na přezkoumání, otestování a nasazení nového bezpečnostního řešení. Vzhledem k tomu, že je k dispozici více než 90 řešení ochrany koncových zařízení, může být obtížné mezi nimi

rozlišovat. Důkladný proces výběru proto zahrnuje definování jasných cílů, využití více zdrojů a metod pro komplexní hodnocení. Při měření účinnosti jednotlivých řešení je důležité posoudit schopnost blokovat zero-day útoky a bránit se proti útokům bez malwaru, například těm, které zneužívají zranitelnosti systému nebo využívají legitimní procesy operačního systému ke škodlivým účelům. Vhodným a nejefektivnějším způsobem, jak vyhodnotit vhodnost produktu je Proof of Concept (PoC) v testovacím prostředí společnosti. Je důležité mít k dispozici potřebné zdroje pro důkladné vyhodnocení a stanovit pevnou dobu trvání, aby se PoC neprotahoval donekonečna. PoC také umožňuje ověřit tvrzení uchazečů/dodavatelů o jejich řešení (Mishra, 2022).

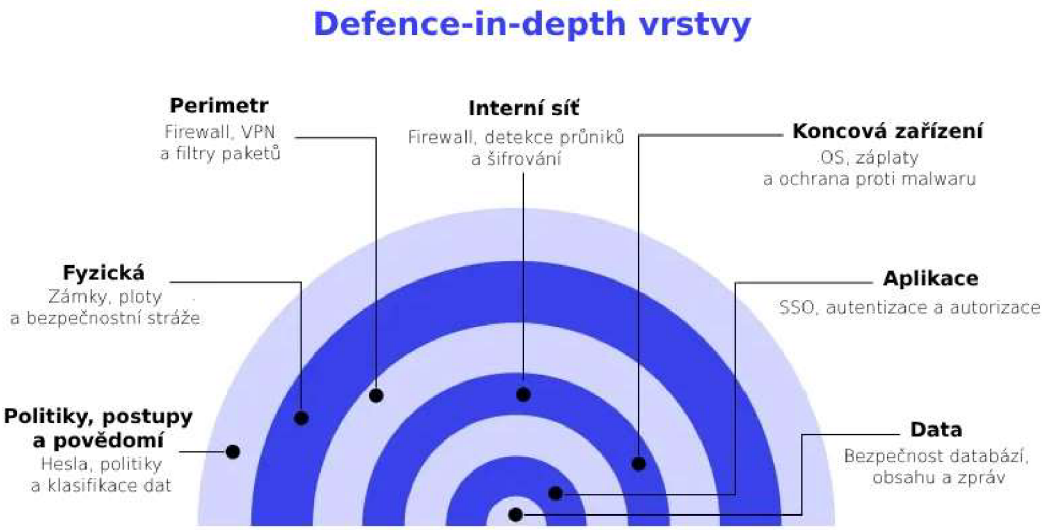
Pro úspěšné nasazení vybraného řešení je důležité nejen vypracování harmonogramu nasazení, ale i následné nastavení a údržba. Instalace a poté udržování softwaru v aktuálním stavu s nejnovějšími záplatami a aktualizacemi je základním principem zabezpečení (Das, 2021). Zatímco menší společnosti to mohou zvládnout s pomocí specializovaných pracovníků, větší organizace čelí náročnému úkolu kvůli obrovskému množství koncových zařízení. Zavedení automatizovaných systémů pro hromadnou instalaci, identifikaci, stahování a nasazování potřebných záplat je pro udržení bezpečnosti v širokém měřítku zásadní. Dalším krokem napojení vybraného řešení je integrace s dalšími systémy jako je například SIEM společnosti, napojení na externí threat intelligence a zavedení procesů pro řešení upozornění generovaných vybraným řešením. Také by mělo dojít k zabezpečení konzole pro správu vícefaktorovým ověřováním. Společnosti by se také neměly spoléhat na výchozí nastavení dodavatele, ale přizpůsobit konfigurace zabezpečení konkrétním potřebám organizace (Trio Team, 2024). Důležitými kroky je školení IT a bezpečnostních pracovníků nejen pro správu bezpečnostního řešení a následné řešení incidentů, ale také průběžný monitoring výkonnosti a nastavení. Pravidelné hodnocení zabezpečení a audity pomohou identifikovat příležitosti ke zlepšení a zajistí, že strategie zabezpečení koncových zařízení společnosti zůstane robustní a bude reagovat na nové hrozby (Mishra, 2022).

3.6 Zasazení EDR v Defence in-depth security

Mughal (2023) definuje hloubkovou obranu je strategický přístup ke kybernetické bezpečnosti, který k ochraně před kybernetickými hrozbami využívá vícevrstvý obranný mechanismus. Tato metoda poskytuje několik vrstev bezpečnostních kontrol a opatření napříč IT infrastrukturou organizace. Pokud dojde k narušení jedné vrstvy, jsou k dispozici další, které udržují celkovou integritu zabezpečení. Tento koncept se často přirovnává

k vrstvám cibule, zobrazeno na Obrázku 3 přičemž každá vrstva poskytuje jedinečnou formu obrany proti potenciálním kybernetickým hrozbám. Tento přístup eliminuje jednotlivá místa selhání v architektuře zabezpečení a snižuje riziko kompletního ohrožení systému s tím, jak se kybernetické hrozby vyvíjejí.

Obrázek 3 Vrstvy modelu Defence in-depth



Zdroj: (Ghost, 2023)

Podle Mughala (2023) se povědomí o bezpečnosti a školení zaměřují na vzdělávání zaměstnanců o rizicích kybernetické bezpečnosti a osvědčených postupech. Pravidelná školení, simulace phishingu a osvětové programy jsou nezbytné pro budování kultury bezpečnosti a posílení postavení zaměstnanců, aby mohli fungovat jako lidský firewall proti kybernetickým hrozbám. Správně nastavené bezpečnostní politiky jako je například délka a komplexita hesla nebo správná klasifikace pomáhají zlepšit bezpečnost. Druhou vrstvou je fyzická bezpečnost, která zahrnuje vše od zámků a plotů, přes ostrahu, bezpečnostní rámy až po kamerové systémy. Zabezpečení perimetru je první linií obrany, jejímž cílem je chránit hranice sítě organizace před vnějšími hrozbami. Zahrnuje firewally, DMZ a systémy detekce narušení, které monitorují a kontrolují příchozí a odchozí síťový provoz. Jeho účelem je fungovat jako strážce brány, který zabraňuje neoprávněnému přístupu a zároveň umožňuje průchod legitimního provozu. Zabezpečení perimetru je klíčovým aspektem zabezpečení interní sítě, které se naproti tomu zaměřuje na ochranu vnitřní síťové infrastruktury před kybernetickými hrozbami. K zabezpečení integrity, důvěrnosti a dostupnosti síťových prostředků a dat se používají opatření, jako jsou interní firewally, virtuální záplaty a posílení

síťových zařízení. Zabezpečení koncových zařízení zajišťuje ochranu jednotlivých zařízení, jako jsou pracovní stanice, notebooky a mobilní zařízení. Zabezpečení koncových bodů zahrnuje používání řešení pro detekci a reakci na koncové body (EDR), antivirového softwaru a technik pro posílení zařízení, které slouží k ochraně před malwarem a dalšími kybernetickými hrozbami zaměřenými na koncová zařízení. Zabezpečení aplikací chrání aplikace před kybernetickými hrozbami zabezpečením softwaru používaného v celé organizaci. Tato vrstva zahrnuje pravidelné skenování zranitelností aplikací, postupy bezpečného kódování a používání webových aplikačních firewallů (WAF) k ochraně před zneužitím. Správa identit a přístupu (Identity and Access Management, IAM) spravuje a řídí přístup uživatelů k systémům a prostředkům. Řešení IAM zahrnují zajišťování uživatelů, vícefaktorovou autentizaci (MFA) a řízení přístupu na základě rolí (RBAC), které zajišťují, že k citlivým informacím a systémům mají přístup pouze oprávnění uživatelé. Cílem zabezpečení dat je chránit citlivé informace před neoprávněným přístupem, manipulací a krádeží. Opatření k zajištění bezpečnosti dat zahrnují šifrování, řešení pro prevenci ztráty dat (DLP) a řízení přístupu k zachování důvěrnosti a integrity citlivých dat.

Mughal (2023) tvrdí, že začlenění EDR řešení do vícevrstvé bezpečnostní strategie může významně posílit obranu organizací proti sofistikovaným a vyvíjejícím se kybernetickým hrozbám. Řešení EDR hrají klíčovou roli ve vrstvě zabezpečení koncových bodů tím, že nabízejí pokročilé možnosti detekce, vyšetřování a reakce na hrozby, které mohou obejít ostatní bezpečnostní opatření. Společně tyto vrstvy vytvářejí komplexní strategii Defense in Depth, která chrání kritická aktiva a citlivé informace organizace před širokou škálou kybernetických hrozeb.

4 Vlastní práce

V této části práce bude popsáno IT prostředí Společnosti a použitý bezpečnostní software. Dále bude popsáno zadání výběrového řízení na nový bezpečnostní software EDR, průběh samotného výběrového řízení, výběr a implementace vybraného produktu.

4.1 O Společnosti

Společnost je členem nadnárodní mateřské zahraniční skupiny působící ve 25 státech. Společnost má přes 250 poboček v rámci České republiky a zaměstnává přes 6000 zaměstnanců po celé České republice.

Oddělení bezpečnosti ve Společnosti hraje klíčovou roli při ochraně digitálního a fyzického majetku Společnosti. Jeho povinnosti přesahují rámec Společnosti i do sesterských a dceřiných společností v České republice v rámci skupiny, takže jeho úloha je pro zachování integrity a bezpečnosti celé skupiny klíčová. Mezi jeho povinnosti patří například řízení provozní bezpečnosti, které zahrnuje nasazení a správu nástrojů kybernetické bezpečnosti, jako je například SIEM (Security Information and Event Management) nebo Endpoint Protection software, provádění pravidelných bezpečnostních auditů a zajištění souladu s předpisy na ochranu dat.

Vzhledem k zodpovědnosti i za sesterské a dceřiné společnosti oddělení zajišťuje konzistentní uplatňování bezpečnostních zásad a postupů ve všech subjektech. To zahrnuje koordinaci s různými týmy IT, standardizaci bezpečnostních opatření a poskytování pokynů v otázkách zabezpečení. Pro zajištění bezpečnosti oddělení často využívá služeb externích odborníků v oblasti kybernetické bezpečnosti.

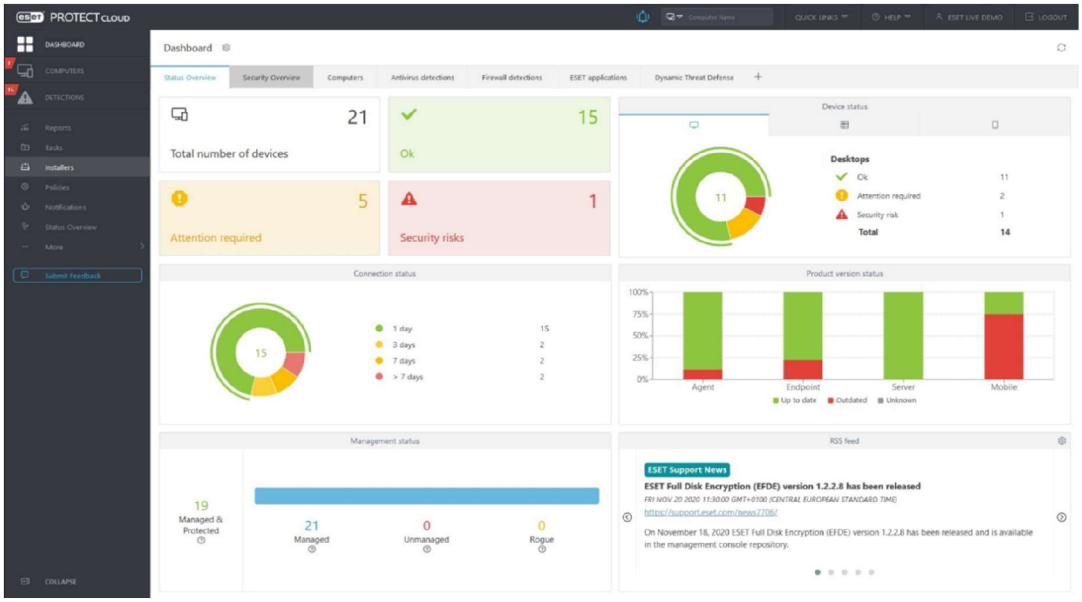
4.1.1 Hardware a software

Oddělení bezpečnosti zajišťuje zabezpečení u více než 6000 uživatelských stanic a více než 1100 serverů. Na 99 % uživatelských stanic je nainstalovaný operační systém Windows 10, zbývající procento zahrnuje testovací stanice s Windows 11 pro plánovaný upgrade, stanice obsluhující legacy software a/nebo hardware a tím pádem využívají starší verze Windows, MacBooky s operačním systém MacOS a vývojářské stanice s Ubuntu. Na šedesáti procentech všech serverů je nainstalován RHEL – Red Hat Enterprise Linux a Debian v různých verzích a na zbývajících 40 % jsou nainstalované různé verze operačního systému Windows Server.

4.1.2 **Bezpečnostní software**

V současné době využívá Společnost pro zabezpečení koncových zařízení a serverů řešení od firmy ESET a z historických důvodů je na několika serverech nainstalovaný antivir od firmy McAfee. Pro správu řešení je využívána management konzole ESET Protect nainstalovaná na on-premise serveru, jejíž hlavní obrazovka je zobrazena na Obrázku 4. Pro zmenšení zátěže je využíván ještě jeden on-premise server jako repositář pro veškeré aktualizační balíčky a instalační balíčky produktů. Management konzole je synchronizovaná s Active Directory jednotlivých společností, což umožňuje nejen granulární přiřazení jednotlivých politik, ale také podrobný přehled, zda jsou zabezpečeny všechny endpointy.

Obrázek 4 Dashboard management konzole ESET Protect



Zdroj: (ESET, 2023b)

Na 99 % všech uživatelských stanic je nainstalován ESET Endpoint Security v různých verzích a na zbývajícím jednom procentu je ESET Endpoint Antivirus v různých verzích. Tento problém s verzemi je dlouhodobě znám a byl způsoben nedostatečnou internetovou konektivitou na některých pobočkách Společnosti.

ESET Endpoint Antivirus je základním produktem společnosti ESET pro firemní prostředí a zaměřuje se především na monitorování v reálném čase a obranu před spektrem kybernetických hrozeb, včetně virů, spyware a ransomware. Jednou z jeho klíčových funkcí je využití pokročilé heuristiky k detekci nových hrozeb, které ještě nemusí být identifikovány v databázích hrozeb. To má zásadní význam pro prevenci útoků nově

vyvinutého malwaru. Navzdory komplexní ochraně je software navržen tak, aby minimalizoval svůj dopad na výkon systému (ESET, 2023a).

ESET Endpoint Security poskytuje oproti ESET Endpoint Antiviru komplexnější přístup ke kybernetické bezpečnosti ve firemním prostředí. Obsahuje navíc další funkce, jako je správa brány firewall, kontrola webu anebo ochranu před botnety. Osobní brána firewall a ochrana proti narušení sítě jsou klíčové pro blokování pokusů o vniknutí a sledování podezřelých síťových aktivit. Funkce kontroly webu podporuje bezpečné prohlížení stránek tím, že blokuje přístup k potenciálně škodlivým webovým stránkám, což je důležitý faktor při prevenci kybernetických incidentů. Ochrana proti botnetům je klíčová pro identifikaci a blokování komunikace z infikovaných zařízení, zabraňuje šíření malwaru a chrání citlivá data (ESET, 2023a).

Na zhruba 10 % serverů jsou nainstalované produkty ESET Server Security for Linux a ESET Server Security for Microsoft Windows Server, zbytek serverů spoléhá na integrovaný Microsoft Defender nebo je bez bezpečnostního software (ESET, 2023d). ESET Server Security for Linux se liší především ochranou Docker kontejnerů, kdy detekuje hrozbu uvnitř kontejneru a on-demand skenem, který vyvolá privilegovaný uživatel (ESET, 2023c). Této funkcionality je ve Společnosti využíváno u webových aplikací pro nahrávání souborů, kdy uživatel nahraje do systému soubor, aplikace zavolá on-demand sken a na základě návratové hodnoty zobrazí uživateli hlášku, zda byl soubor úspěšně nahrán nebo došlo k chybě a je potřeba jej nahrát znovu.

Jednotlivé endpointy jsou zařazeny do skupin, které se načítají z Active Directory a na které jsou následně aplikovány bezpečnostní politiky. Synchronizace s Active Directory probíhá každou hodinu pomocí úlohy v management konzoli. Dále jsou vytvořené dynamické skupiny, které přiřazují další politiky na základě operačního systému. Bezpečnostní politiky mají různé nastavení pro notebooky a stolní počítače uživatelů, kdy například blokují přístup na webové stránky nebo blokují zobrazení upozornění bezpečnostního produktu, která jsou odesílána pouze do management konzole. Přístup do konzole je omezen na vybrané administrátory serverů a techniky uživatelské podpory, kteří mají granulárně nastavená oprávnění pro práci pouze se skupinami zařízení, která spravují. Hlavními správci ESET Protect management konzole jsou členové Oddělení bezpečnosti, kteří mají plná oprávnění a zodpovídají za nastavení jednotlivých politik, aktualizace management konzole a řešení nálezů.

4.2 Výběrové řízení

V souvislosti s vývojem kybernetické bezpečnosti zahájila Společnost výběrové řízení na nové Endpoint Detection and Response (EDR) řešení. K tomuto rozhodnutí vedly především dva zásadní faktory: blížící se konec platnosti licencí stávajícího bezpečnostního řešení a dynamický vývoj kybernetických hrozeb, které vyžadují pokročilou ochranu.

Vypršení platnosti licencí stávajícího bezpečnostního řešení představuje pro Společnost příležitost k přehodnocení potřeb společnosti v oblasti kybernetické bezpečnosti. Vypršení platnosti licencí je pro organizace běžným podnětem k přezkoumání jejich stávajících strategií kybernetické bezpečnosti a otevírá se tak prostor pro vyhodnocení novějších, pokročilejších možností na trhu. Vzhledem k rychlému pokroku v technologii EDR by setrvání u stávajícího řešení z důvodu obnovení licence mohlo potenciálně způsobit, že organizace bude zranitelná vůči novějším typům kybernetických útoků.

Prostředí kybernetických hrozeb se neustále vyvíjí a pravidelně se objevují nové typy sofistikovaných útoků. Společnost si uvědomuje potřebu výběru EDR řešení, které dokáže nejen reagovat na současné hrozby, ale také se přizpůsobit budoucím výzvám. Dnešní EDR řešení jsou navržena tak, aby šla nad rámec reaktivních opatření a poskytovala proaktivní vyhledávání hrozeb, pokročilou analytiku a možnosti automatické reakce. Tento prozíravý přístup je nezbytný pro organizace, které musí chránit citlivá data, dodržovat předpisy a udržovat provozní integritu před stále složitějšími a skrytějšími kybernetickými hrozbami. Nové EDR řešení zvýší schopnost Společnosti efektivněji a účinněji odhalovat, vyšetřovat a reagovat na kybernetické incidenty.

Vypsání výběrového řízení na nové EDR řešení je strategické rozhodnutí, které prokazuje závazek udržovat robustní kybernetickou bezpečnost a umožňuje vyhodnotit různá nejmodernější EDR řešení s ohledem na faktory, jako je technologický pokrok, kompatibilita se stávající IT infrastrukturou a celková nákladová efektivita. Tento proces je rozhodující pro výběr řešení, které nejen splňuje současné bezpečnostní požadavky, ale je také škálovatelné a přizpůsobitelné budoucím potřebám.

4.2.1 Parametry výběrového řízení

Výběrové řízení bylo vypsáno ve spolupráci s Oddělením nákupu s následujícími parametry a technickými požadavky:

- uchazeči musí podepsat smlouvu o mlčenlivost;

- nabídková cena bude rozdělena na dvě části, objem licence a servisní podpora. Pokud bude nabídka obsahovat více variant, je nutné, aby byly řádně odlišeny a byla patrná základní cena.

Technická kvalifikace:

- uchazeč musí doložit alespoň dvě relevantní významné a úspěšně realizované zakázky;
- uchazeč musí doložit, že je oficiálním partnerem výrobce nebo lokálním distributorem pro Českou republiku.

Technické požadavky – obecné:

- povolené technologie pro nabídky byly omezeny na SentinelOne, Trend Micro, Palo Alto Networks, Microsoft a Bitdefender;
- objem licencí v nabídce bude v objemu 6400 uživatelských stanic a 1400 serverů (fyzické a virtuální).

Technické požadavky – nefunkční:

Mandatorní podpora následujících OS a virtualizačních prostředí:

- MS Windows 10 v20H2 a novější;
- MacOS;
- MS Windows Server 2012-2019;
- Red Hat Enterprise Linux 6, 7; Debian 9-10;
- VMware Sphere.

Mandatorní možnost integrace s následujícími technologiemi:

- IBM QRadar.

Doporučená možnost integrace s následujícími technologiemi:

- ServiceNow;
- Firewally výrobců s významným podílem na trhu (CheckPoint, Cisco, Fortinet, Palo Alto).

Požadavky na distribuci agentů:

- Kompatibilita s SCCM 2107;
- Kompatibilita s Ansible pro Linux agenty;
- Distribuce pomocí MSI balíčku s případnou parametrizací pro silent/bezobslužnou instalaci.

Technické požadavky – funkční:

Řešení obecně pokrývá funkcionality spadající do oblasti jak Endpoint Protection Platform (EPP), tak Endpoint Detection and Response (EDR) a Extended Detection and Response (XDR) – a to buď v rámci jednoho produktu, nebo v rámci plynule integrovatelných modulů. Nabídka může obsahovat více variant řešení v rámci jedné technologické platformy.

Požadovány jsou zejména následující funkční parametry/vlastnosti:

- vysoká spolehlivost detekce relevantních událostí (bude hodnoceno na základě výsledků dané technologie v testu MITRE 2021 Carbanak+FIN7 ATT&CK Evaluation);
- jednotná centrální konzole pro řešení bezpečnostních incidentů, s minimalizovanou potřebou pro přecházení mezi komponenty/prostředími řešení;
- integrace modelu MITRE ATT&CK v rámci systému řešení incidentů, včetně automatizovaného real-time mapování událostí dle daného modelu;
- přehledná vizualizace probíhajícího incidentu v rámci centrální konzole;
- široké spektrum možností reakce na probíhající incident na stanicích/serverech s agentem;
- možnost retence dat minimálně 3 měsíce, preferovaně až 12 měsíců;
- detekce zranitelností na stanicích/serverech s agentem;
- možnost Device Control pro management užívání externích médií na stanicích;
- sandbox funkcionalita pro automatizovanou analýzu detekovaných vzorků;
- přehledné mapování spuštěných procesu v rámci vyšetřování bezpečnostního incidentu;
- možnost napojení externích zdrojů Threat Intelligence;
- možnost vytváření vlastních (custom) pravidel pro vyhledávání IoC;
- možnosti ochrany zranitelných verzí OS/aplikací např. virtual patchingem nebo jiným způsobem.

4.2.2 Průběh výběrového řízení

První kolo výběrového řízení na řešení EDR bylo zásadním krokem v úsilí Společnosti o zlepšení její kybernetické bezpečnosti. Této fáze se zúčastnilo osm uchazečů,

kteří představili hodnotící komisi své produkty. Jednomu z uchazečů bylo umožněno zúčastnit se výběrového řízení s řešením, které nebylo dříve preferováno. Toto rozhodnutí zahrnout dříve méně preferovanou možnost značí ochotu Společnosti prozkoumat všechny možnosti, zůstat otevřený různým technologickým řešením a snahu zajistit co nejlepší možný výsledek při výběru nového EDR řešení. Jedním z pozoruhodných aspektů tohoto kola byly značné rozdíly v kvalitě prezentací, které uchazeči přednesli. Tyto rozdíly sahaly od velmi precizních a komplexních ukázek až po ty, které byly méně přesvědčivé a poněkud málo podrobné. Tato rozdílná kvalita prezentací významně ovlivnila schopnost Společnosti důsledně vyhodnotit možnosti jednotlivých řešení EDR. Pro organizaci, která hledá řešení, jež by přesně odpovídalo jejím specifickým bezpečnostním potřebám, byla srozumitelnost a hloubka těchto prezentací rozhodující pro usnadnění informovaného rozhodovacího procesu. Uchazeči ve svých prezentacích zdůrazňovali technické přednosti svých řešení EDR, včetně takových aspektů, jako je detekce hrozeb v reálném čase, schopnosti reakce a integrace se stávajícími IT systémy. Účinnost těchto prezentací se lišila, někteří dodavatelé poskytli podrobný náhled na funkce svých produktů, jiní nedokázali efektivně informovat o výhodách svého řešení.

Po prezentacích předložili uchazeči své cenové kalkulace v Příloze 3. V těchto předložených kalkulacích se do jisté míry projevila rozdílná kvalita prezentací a dva z osmi uchazečů nebyli vybrán do dalšího kola, jelikož nabídka Uchazeče 6 byla obsahově totožná, nicméně se lišila vyšší cenou. Uchazeč 4 nepostoupil z důvodu kvalitativně horší nabídky v porovnání s Uchazečem 1 totožné technologie SentinelOne a podhodnocené implementaci, což bylo patrné z porovnání s ostatními uchazeči. Zároveň toto rozhodnutí vedlo k tomu, že každou technologii zastupovala pouze jedna nabídka, což zefektivnilo výběrový proces a umožnilo cílenější hodnocení každého navrženého řešení.

Ve druhém kole Společnost uspořádala sérii technických seminářů se šesti zbývajícími uchazeči. Tyto workshopy měly zásadní význam pro ověření technických možností každého řešení a poskytly příležitost k hloubkovému praktickému přezkoumání. Cílem bylo pečlivě posoudit, jak jednotlivá řešení odpovídají konkrétním technickým požadavkům stanovenými Společností na začátku výběrového řízení. Tyto technické workshopy se ukázaly jako vysoce informativní a užitečné v procesu hodnocení. Ukázaly, že řešení od Palo Alto, SentinelOne a Trend Micro úspěšně splňují všechna stanovená kritéria a prokázala robustnost a soulad s technickými požadavky. Workshopy naopak odhalily, že řešení Bitdefender, Microsoft a CheckPoint splňují technické standardy

společnosti méně úspěšně. Tento rozdíl ve výkonu a schopnostech byla rozhodujícím faktorem v následném rozhodovacím procesu.

Pro objektivní vyhodnocení tohoto kola použila společnost jedinou hodnotící matici, která kombinovala cenové i technické aspekty návrhů. Aby se zohlednil zvýšený důraz na technické schopnosti řešení, byla hodnotící matice vážena s 60 % důrazem na kvalitu a 40 % na cenu. Toto váhové schéma zdůraznilo upřednostnění technické kvality v tomto kole. Bylo však dohodnuto, že v dalších kolech by se váhy mohly upravit tak, aby se větší váha přikládala ceně a vyvážila se tak celková hodnota každého návrhu.

Hodnocení jednotlivých workshopů byla zanesena do hodnotící matice, vyobrazené v Tabulce 2, kde byly použity koeficienty pro označení důležitosti daného požadavku. Každý požadavek byl ohodnocen bodovou stupnicí 0-3 s následujícím významem:

0 - funkcionalita chybí / nevyhovuje

1 - funkcionalita částečně vyhovující

2 - funkcionalita vyhovující

3 - funkcionalita nadstandardní

Toto bodové ohodnocení bylo vynásobeno koeficientem pro výsledné hodnocení konkrétního požadavku a následně byly sečteny všechny výsledné hodnocení u posuzovaného produktu, tedy obdoba metody váženého součtu. Také bylo vypočteno maximální možné ohodnocení pro procentuální ohodnocení jednotlivých produktů.

Tabulka 2 Technické hodnocení během workshopů

Položka hodnocení	Koef.	Uchazeč 1 / SentinelOne		Uchazeč 2 / Palo Alto		Uchazeč 3 / Trend Micro		Uchazeč 5 / Bitdefender		Ucahzeč 7 / Microsoft		Uchazeč 8 / Check Point		Maximální možné	
Vysoká spolehlivost detekce relevantních událostí (bude hodnoceno na základě výsledků dané	3	3	9	3	9	3	9	2	6	2	6	2	6	3	9
Jednotná centrální konzole pro řešení bezpečnostních incidentů, s minimalizovanou	3	3	9	2	6	2	6	2	6	1	3	2	6	3	9
Integrace modelu MITRE ATT&CK v rámci systému řešení incidentů, včetně automatizovaného real-time	1	3	3	3	3	3	3	2	2	2	2	3	3	3	3
Přehledná vizualizace probíhajícího incidentu v rámci centrální konzole.	2	3	6	1	2	3	6	2	4	2	4	1	2	3	6
Široké spektrum užívaných senzorů/zdrojů událostí/telemetrie (včetně např. síťové sondy).	2	1	2	1	2	2	4	2	4	1	2	0	0	3	6
Široké spektrum možností reakce na probíhající incident na stanicích/serverech s agentem.	3	3	9	3	9	3	9	2	6	2	6	1	3	3	9
Možnost retence dat minimálně 3 měsíce, preferovaně až 12 měsíců.	2	2	4	2	4	2	4	1	2	1	2	2	4	3	6
Detekce zranitelností na stanicích/serverech s agentem.	1	1	1	2	2	3	3	2	2	1	1	2	2	3	3
Možnost Device Control pro management užívání externích médií na stanicích.	1	2	2	1	1	2	2	1	1	0	0	3	3	3	3
Sandbox funkcionalita pro automatizovanou analýzu detekovaných vzorků.	2	0	0	2	4	2	4	2	4	1	2	1	2	3	6
Přehledné mapování spuštěných procesu v rámci vyšetřování bezpečnostního incidentu.	1	2	2	2	2	2	2	2	2	2	2	1	1	3	3
Možnost napojení externích zdrojů Threat Intelligence.	2	1	2	2	4	3	6	0	0	0	0	0	0	3	6
Možnost vytváření vlastních (custom) pravidel pro vyhledávání IoC.	2	1	2	2	4	2	4	2	4	2	4	2	4	3	6
Možnosti ochrany zranitelných verzí OS/aplikací např. virtual patchingem nebo jiným způsobem.	1	1	1	2	2	3	3	0	0	1	1	1	1	3	3
Výsledky demonstrací a ukázek jednotlivých zadaných use cases během workshopu	5	2	10	2	10	2	10	1	5	2	10	2	10	3	15
Kvalita přípravy nabídky a workshopu	1	2	2	2	2	3	3	1	1	2	2	2	2	3	3
Preference budoucích operátorů	1	3	3	2	2	2	2	1	1	1	1	3	3	3	3
			67		68		80		50		48		52		99
Procentuální hodnocení z maximálního možného počtu bodů			**67,7%**		**68,7%**		**80,8%**		**50,5%**		**48,5%**		**52,5%**		

Zdroj: (Vlastní zpracování, 2022)

Pro ověření správnosti byla tato hodnotící matice převedena na druhou matici, vyobrazené v Tabulce 3, kde byla použita zjednodušená metoda váženého součtu. V kontextu vícekriteriálního hodnocení variant podle Šmerka (2014), metoda váženého součtu využívá znalosti vah kritérií. Jako kompromisní je vybrána ta varianta, která maximalizuje součet součinů vah kritérií a odpovídajících hodnot z normalizované kriteriální matice. Prvním krokem bylo převedení koeficientů na váhy pomocí tohoto vzorce:

$$v_i = \frac{k_i}{\{\sum k_j\}} \tag{1}$$

Kde v_i je normalizovaná váha i-tého koeficientu, k_i je i-tý koeficient a $\sum k_j$ je součet všech koeficientů, kde j prochází všemi koeficienty a $\sum v_i$ se musí rovnat 1. Druhým krokem byl výpočet samotného váženého součtu pomocí vzorce:

$$X_k = \sum_{j=1}^{k} v_j r_{ij} \rightarrow \max \tag{2}$$

Kde X_k je vážený součet pro variantu i, v_j je váha kritéria j a r_{ij} je hodnota varianty i podle kritéria j.

Tabulka 3 Tabulka technického hodnocení během workshopů, koeficienty převedeny na váhy

Položka hodnocení	Koef.	Váha	Uchazeč 1 / SentinelOne		Uchazeč 2 / Palo Alto		Uchazeč 3 / Trend Micro		Uchazeč 5 / Bitdefender		Ucahzeč 7 / Microsoft		Uchazeč 8 / Check Point		Maximální možné ohodnocení	
Vysoká spolehlivost detekce relevantních událostí (bude hodnoceno na základě výsledků dané technologie v testu MITRE 2021 Carbanak+FIN7 ATT&CK Evaluation).	3	0,091	3	0,273	3	0,273	3	0,273	2	0,182	2	0,182	2	0,182	3	0,273
Jednotná centrální konzole pro řešení bezpečnostních incidentů, s minimalizovanou potřebou pro přecházení mezi komponenty/prostředími řešení.	3	0,091	3	0,273	2	0,182	2	0,182	2	0,182	1	0,091	2	0,182	3	0,273
Integrace modelu MITRE ATT&CK v rámci systému řešení incidentů, včetně automatizovaného real-time mapování událostí dle daného modelu.	1	0,030	3	0,091	3	0,091	3	0,091	2	0,061	2	0,061	3	0,091	3	0,091
Přehledná vizualizace probíhajícího incidentu v rámci centrální konzole.	2	0,061	3	0,182	1	0,061	3	0,182	2	0,121	2	0,121	1	0,061	3	0,182
Široké spektrum užívaných senzorů/zdrojů událostí/telemetrie (včetně např. síťové sondy).	2	0,061	1	0,061	1	0,061	2	0,121	2	0,121	1	0,061	0	0,000	3	0,182
Široké spektrum možností reakce na probíhající incident na stanicích/serverech s agentem.	3	0,091	3	0,273	3	0,273	3	0,273	2	0,182	2	0,182	1	0,091	3	0,273
Možnost retence dat minimálně 3 měsíce, preferovaně až 12 měsíců.	2	0,061	2	0,121	2	0,121	2	0,121	1	0,061	1	0,061	2	0,121	3	0,182
Detekce zranitelností na stanicích/serverech s agentem.	1	0,030	1	0,030	2	0,061	3	0,091	2	0,061	1	0,030	2	0,061	3	0,091
Možnost Device Control pro management užívání externích médií na stanicích.	1	0,030	2	0,061	1	0,030	2	0,061	1	0,030	0	0,000	3	0,091	3	0,091
Sandbox funkcionalita pro automatizovanou analýzu detekovaných vzorků.	2	0,061	0	0,000	2	0,121	2	0,121	2	0,121	1	0,061	1	0,061	3	0,182
Přehledné mapování spuštěných procesu v rámci vyšetřování bezpečnostního incidentu.	1	0,030	2	0,061	2	0,061	2	0,061	2	0,061	2	0,061	1	0,030	3	0,091
Možnost napojení externích zdrojů Threat Intelligence.	2	0,061	1	0,061	2	0,121	3	0,182	0	0,000	0	0,000	0	0,000	3	0,182
Možnost vytváření vlastních (custom) pravidel pro vyhledávání IoC.	2	0,061	1	0,061	2	0,121	2	0,121	2	0,121	2	0,121	2	0,121	3	0,182
Možnosti ochrany zranitelných verzí OS/aplikací např. virtual patchingem nebo jiným způsobem.	1	0,030	1	0,030	2	0,061	3	0,091	0	0,000	1	0,030	1	0,030	3	0,091
Výsledky demonstrací a ukázek jednotlivých zadaných use cases během workshopu	5	0,152	2	0,303	2	0,303	2	0,303	1	0,152	2	0,303	2	0,303	3	0,455
Kvalita přípravy nabídky a workshopu	1	0,030	2	0,061	2	0,061	3	0,091	1	0,030	2	0,061	2	0,061	3	0,091
Preference budoucích operátorů	1	0,030	3	0,091	2	0,061	2	0,061	1	0,030	1	0,030	3	0,091	3	0,091
		1		2,030		2,061		2,424		1,515		1,455		1,576		3
Procentuální hodnocení z maximálního možného počtu bodů				67,7%		68,7%		80,8%		50,5%		48,5%		52,5%		

Zdroj: (Vlastní zpracování, 2022)

Následně bylo procentuální hodnocení každého produktu dosazeno do celkové matice hodnocení druhého kola, vyobrazené v Tabulce 4, kde byla zohledněna i cena daného řešení a byla použita metoda normalizace cen. K té byl využit vzorec:

$$C_{norm,i} = \frac{C_{min}}{C_i} \tag{3}$$

Kde Cnorm,i je normalizovaná cena i-té nabídky, Cmin je nejnižší cena ze všech nabídek a Ci je cena i-té nabídky. Následně tato normalizovaná cena byla vynásobena 40 % a sečteny vážené hodnoty.

Tabulka 4 Celkové hodnocení uchazečů po druhém kole výběrového řízení

			Uchazeč 1	Uchazeč 2	Uchazeč 3	Uchazeč 5	Uchazeč 7	Uchazeč 8
Hodnocená položka	Váha		SentinelOne	Palo Alto	Trend Micro	Bitdefender	Microsoft	CheckPoint
Cena	40%	*Absolutní hodnota (cena za 3 roky vč. implementace)*	*22 781 690,87 Kč*	*26 079 563,40 Kč*	*28 616 033,80 Kč*	*21 405 868,00 Kč*	*19 888 624,80 Kč*	*20 961 565,68 Kč*
		Vážená hodnota	**34,9%**	**30,5%**	**27,8%**	**37,2%**	**40,0%**	**38,0%**
Technické hodnocení	60%	*Absolutní hodnota (z listu "Matice tech. Hodnocení")*	*67,7%*	*68,7%*	*80,8%*	*50,5%*	*48,5%*	*52,5%*
		Vážená hodnota	**40,6%**	**41,2%**	**48,5%**	**30,3%**	**29,1%**	**31,5%**
Celkové hodnocení (součet vážených hodnot)			**75,5%**	**71,7%**	**76,3%**	**67,5%**	**69,1%**	**69,5%**

Zdroj: (Vlastní zpracování, 2022)

Na základě Celkového hodnocení bylo rozhodnuto, že do dalšího kola postoupí první tři uchazeči. Zbývajícím uchazečům bylo oznámeno ukončení účasti ve výběrovém řízení. Postupující uchazeči byli požádáni o úpravu cenových nabídek po úpravě zadání ze strany Společnosti. Změny byly následující: Licence Endpoint (6400) → Licence Endpoint (6600), Licence Server (1400) → Licence Server (1500), Jiné (7800) → Jiné (8100). O tomto navýšení počtu licencí bylo rozhodnuto kvůli případnému nárůstu koncových zařízení v budoucnu.

Do dalšího kola, kterým bude provedení Proof of Concept (PoC), postoupí pouze dva uchazeči. Ti budou vybráni na základě aktualizovaných cenových nabídek v Tabulce 5. Také bylo rozhodnuto, že se změní váhy pro jednotlivá hodnocení. Cenová nabídka nyní bude mít váhu 60 % a Technické hodnocení 40 %, vyobrazené v Tabulce 6, v souladu s usnesením hodnotící komise. Toto rozhodnutí bylo přijato na základě velmi podobných hodnot Technického hodnocení jednotlivých produktů a s cílem jednat jako zodpovědný hospodář při výběru řešení s nejvýhodnějším poměrem ceny a kvality.

Tabulka 5 Aktualizované cenové nabídky před třetím kolem

	Uchazeč 1	Uchazeč 2	Uchazeč 3
Řešení	**SentinelOne**	**Palo Alto**	**Trend Micro**
Dílčí ceny při nákupu na jeden rok	cena v Kč vč. DPH	cena v Kč vč. DPH	cena v Kč vč. DPH
Licence Endpoint (6600ks)	3 716 584,87 Kč	4 877 340,24 Kč	2 115 768,37 Kč
Licence Server (1500ks)	1 329 641,51 Kč		2 094 974,67 Kč
Jiné (8100ks)	3 661 474,66 Kč	4 381 290,94 Kč	5 337 335,35 Kč
Implementace	460 405,00 Kč	1 835 095,68 Kč	387 200,00 Kč
Servisní podpora - 1 rok	747 054,00 Kč	387 684,00 Kč	464 640,00 Kč
Celkem za 1. rok	**9 915 160,04 Kč**	**11 481 410,85 Kč**	**10 399 918,39 Kč**
Licence Endpoint (6600ks)	10 449 178,17 Kč	12 193 350,59 Kč	5 499 906,99 Kč
Licence Server (1500ks)	3 732 814,00 Kč		5 443 892,44 Kč
Jiné (8100ks)	10 346 269,44 Kč	12 440 515,04 Kč	15 380 716,26 Kč
Implementace	460 405,00 Kč	1 835 095,68 Kč	387 200,00 Kč
Servisní podpora - 3 roky	2 241 162,00 Kč	1 163 052,00 Kč	1 393 920,00 Kč
Celkem za 3 roky	**27 229 828,61 Kč**	**27 632 013,31 Kč**	**28 105 635,69 Kč**

Zdroj: (Vlastní zpracování, 2022)

Tabulka 6 Celkové hodnocení po aktualizaci cen

			Uchazeč 1	Uchazeč 2	Uchazeč 3
Hodnocená položka	**Váha**		**SentinelOne**	**Palo Alto**	**Trend Micro**
Cena	**60%**	*Absolutní hodnota (cena za 3 roky vč. Implementace a servisu)*	*27 229 828,61 Kč*	*27 632 013,31 Kč*	*28 105 635,69 Kč*
		Vážená hodnota	**60,0%**	**59,1%**	**58,1%**
Technické hodnocení	**40%**	*Absolutní hodnota (z listu "Matice tech. Hodnocení")*	*67,7%*	*68,7%*	*80,8%*
		Vážená hodnota	**27,1%**	**27,5%**	**32,3%**
Celkové hodnocení (součet vážených hodnot)			**87,1%**	**86,6%**	**90,5%**

Zdroj: (Vlastní zpracování, 2022)

Hodnotící komise rozhodla o nákupu EDR řešení na tři roky, proto do porovnání vstoupila cena za tři roky. Na základě aktualizovaného Celkového hodnocení postoupili do dalšího kola Uchazeč 1 a Uchazeč 3. Uchazeč 2 byl informován o nepostoupení do dalšího kola, avšak byl požádán o setrvání ve výběrovém řízení pro případ, že PoC jednoho z postupujících uchazečů nebude úspěšné. Hodnotící komise také rozhodla o vytvoření kriteriálního hodnocení PoC, o které bude rozšířena výsledná matice Celkového hodnocení.

Cílem PoC bylo vyhodnotit praktické nasazení a účinnost jednotlivých řešení v prostředí Společnosti. Každé řešení bylo nasazeno v několika prostředích ve Společnosti, včetně týmu oddělení bezpečnosti, malé skupiny správců systému, testovacích serverů a virtuálních počítačů. Tento přístup zajistil komplexní hodnocení napříč různými skupinami uživatelů a technickými prostředími. Délka testování každého řešení byla jeden týden.
PoC se zaměřilo na několik klíčových kritérií pro měření účinnosti jednotlivých řešení:
Implementace / Distribuce: Jak snadný a efektivní byl proces nasazení.
Detekce: Schopnost identifikovat potenciální hrozby a skutečné vzorky malware.
Response: Účinnost reakce na skutečné vzorky malware.
Administrace: Jak snadno lze jednotlivá řešení spravovat a konfigurovat.
Integrace: Jak se jednotlivá řešení integrují do stávající infrastruktury IT.
Sekundární funkce: Hodnocení dalších funkce a vlastností.
Podpora dodavatele: Úroveň a účinnost podpory dodavatele.

K objektivnímu porovnání obou řešení byl použit jednoduchý bodový systém, jelikož všechna kritéria měla stejnou váhu. Za každé hodnotící kritérium získalo řešení, které prokázalo vyšší kvalitu nebo výkon, 1 bod. Pokud byla obě řešení vyhodnocena jako stejně kvalitní pro dané kritérium, získalo každé řešení 1 bod. Tato metoda poskytla jasný, kvantifikovatelný způsob, jak posoudit silné a slabé stránky každého řešení u více kritérií.

Po sečtení všech bodů v Tabulce 7 bylo vypočteno procentuální hodnocení, které bylo dosazeno do výsledné matice Celkového hodnocení.

Tabulka 7 Hodnocení jednotlivých kritérií během Proof of Concept

Oblast	SentinelOne / Uchazeč 1	Trend Micro / Uchazeč 3
Implementace/distribuce	1	0
Detekce	1	0
Response	1	0
Administrace	1	0
Integrace	1	1
Druhotné funkce	1	1
Podpora partnera	1	1
Součet	**7**	**3**
Hodnocení v %	**100%**	**43%**

Zdroj: (Vlastní zpracování, 2022)

PoC přinesl několik zásadních poznatků. Zejména pro řešení Trend Micro odhalilo, že plně nesplňuje požadavky společnosti, což bylo překvapivé zjištění vzhledem k předchozím informacím získaných během workshopu. Hlavními problémy, které členové týmu identifikovali, byla složitost způsobená použitím tří konzolí pro správu, což ztěžovalo proces administrace a nedostatečné schopnosti detekce reálného malware. Naproti tomu řešení SentinelOne prokázalo očekávané komplexní možnosti. Významným přínosem řešení SentinelOne byla jeho zjednodušená správa, kterou usnadňovala jediná konzole pro správu, ale také především možnosti hloubkové analýzy a investigace včetně plnohodnotného remote shellu nebo stažení podezřelých souborů ze systémů využívající operační systémy Windows. Velkým přínosem na systémech Windows byla také funkce Rollback, která při využití funkce Shadow Copies umožňuje vrátit změny provedené ransomware.

Proof of Concept fáze výběrového řízení byla rozhodující pro zajištění toho, aby společnost vybrala řešení EDR, které splňuje její potřeby jak z hlediska technických možností, tak z hlediska snadného používání díky nasazení v reálném prostředí Společnosti.

Před konečným rozhodnutím byli uchazeči požádáni o aktualizaci cenových nabídek s cílem získat co nejlepší cenovou nabídku a tyto ceny z Tabulky 8 byly následně přeneseny do výsledné matice Celkového hodnocení.

Tabulka 8 Poslední aktualizace cen od uchazečů

	Uchazeč 1	Uchazeč 3
Řešení	**SentinelOne**	**Trend Micro**
Dílčí ceny při nákupu na jeden rok	cena v Kč vč. DPH	cena v Kč vč. DPH
Licence Endpoint (6600ks)	3 426 617,84 Kč	1 994 199,02 Kč
Licence Server (1500ks)	1 223 324,07 Kč	1 973 630,48 Kč
Jiné (8100ks)	3 387 220,53 Kč	5 057 166,12 Kč
Implementace	428 176,65 Kč	387 200,00 Kč
Servisní podpora - 1 rok	660 660,00 Kč	464 640,00 Kč
Celkem za 1. rok	**9 125 999,09 Kč**	**9 876 835,62 Kč**
Licence Endpoint (6600ks)	9 613 696,06 Kč	5 161 592,79 Kč
Licence Server (1500ks)	3 426 506,31 Kč	5 109 023,65 Kč
Jiné (8100ks)	9 557 681,06 Kč	14 433 282,29 Kč
Implementace	428 176,65 Kč	387 200,00 Kč
Servisní podpora - 3 roky	1 981 980,00 Kč	1 393 920,00 Kč
Celkem za 3 roky	**25 008 040,09 Kč**	**26 485 018,73 Kč**

Zdroj: (Vlastní zpracování, 2022)

Pro Celkové hodnocení v Tabulce 9, byla ceně ponechána váha 60 % a pro Technické hodnocení byla rozdělena na 20 % pro hodnocení informací z workshopu a 20 % pro hodnocení z PoC. Hodnotící komice přijala rozdělení váhy Technického hodnocení, aby lépe reflektovalo dvě různá hodnocení.

Tabulka 9 Celkové hodnocení po Proof of Concept

			Uchazeč 1	Uchazeč 3
Hodnocená položka	**Váha**		**SentinelOne**	**Trend Micro**
Cena	**60%**	*Absolutní hodnota (cena za 3 roky vč. Implementace a servisu)*	*25 008 040,09 Kč*	*26 485 018,73 Kč*
		Vážená hodnota	**60,0%**	**56,7%**
Technické hodnocení - workshop	**20%**	*Absolutní hodnota (z listu "Matice tech. Hodnocení")*	*67,7%*	*80,8%*
		Vážená hodnota	**13,5%**	**16,2%**
Technické hodnocení - PoC	**20%**	*Absolutní hodnota (z listu "Tech. hodn. po PoC")*	*100,0%*	*42,9%*
		Vážená hodnota	**20,0%**	**8,6%**
Celkové hodnocení (součet vážených hodnot)			**93,5%**	**81,4%**

Zdroj: (Vlastní zpracování, 2022)

Na základě Celkového rozhodnutí bylo rozhodnuto o pořízení řešení SentinelOne od Uchazeče 1. Uchazeč 3 byl informován o výsledku výběrového řízení.

4.3 Nasazení vybraného EDR řešení

Proces výběrového řízení byl úspěšně zakončen. Po podpisu všech relevantních smluv a zkompletování procesu nákupu došlo k transformaci statutu Uchazeče 1 na status Dodavatele. Během přípravy implementace bylo rozhodnuto, že nejprve dojde k nasazení EDR řešení na koncové stanice uživatelů a poté bude EDR postupně nasazováno na servery. S Dodavatelem byly domluvené pravidelné schůzky online formou dvakrát týdně, na nichž byly diskutovány změny a problémy, které vyvstaly v průběhu jednotlivých fází nasazení.

4.3.1 Nasazení EDR na koncové stanice

První fází projektu výměny současného bezpečnostního řešení bylo nasazení řešení SentinelOne EDR na více než 6 000 koncových stanic napříč celou Společností, a to včetně všech sesterských a dceřiných společností. Klíčovým ukazatelem výkonnosti (KPI) pro toto nasazení bylo dosažení 98% pokrytí koncových stanic do jednoho měsíce od začátku nasazení. Tento ambiciózní cíl odrážel závazek Společnosti ke komplexnímu pokrytí kybernetické bezpečnosti.

V rámci přípravy na nasazení bylo provedeno několik klíčových kroků. Prvním z nich bylo vytvoření skupin v konzoli pro správu. Vytvořené skupiny byly rozdělené podle názvu společnosti, aby se zjednodušilo nasazení a správa. Každá ze skupin měla svůj vlastní token, pomocí kterého došlo k přiřazení agentů do požadovaných skupin. Druhým krokem byla příprava samotného procesu a časového rámce nasazení, jelikož během něj muselo dojít k odinstalaci současného řešení, restartování koncové stanice, instalace agenta SentinelOne a opětovné restartování koncové stanice. Třetím krokem byla potřeba připravit komunikace směřovanou na uživatele, aby byli informováni o připravovaném nasazení a možných problémech, které mohou vyvstat během tohoto procesu. Školení uživatelů nebylo potřeba, jelikož upozornění, která mohla být uživatelům zobrazena, byla vypnuta. Veškerá upozornění uvidí správce v management konzoli a uživatel nebude rušen při práci.

Nasazení bylo strategicky provedeno ve fázích s využitím stávající struktury v nástroji System Center Configuration Manager (SCCM). První fáze byla zaměřena na testovací skupinu pečlivě vybranou tak, aby zahrnovala uživatele z každého oddělení, čímž bylo zajištěno široké a reprezentativní testovací prostředí. U dceřiných společností, které ještě nebyly integrovány s SCCM nebo používaly operační systému MacOS a Ubuntu, vedly nasazení místní IT týmy.

Po úspěšné testovací fázi trvalo nasazení na zbývající koncové stanice přibližně tři týdny. Toto rychlé provedení bylo způsobeno efektivní spoluprací s jednotlivými lokálními IT odděleními. Navzdory celkovému úspěchu se vyskytly drobné problémy, přičemž přibližně 30 koncových stanic zůstalo nezapojeno z důvodu problémů s připojením nebo dlouhodobé nečinnosti. Několik desítek koncových stanic také vyžadovalo specializovaný odinstalační nástroj ESET kvůli neshodě verzí nebo poškozeným instalacím. Tyto problémy se podařilo vyřešit během následujících týdnů. Počet problematických stanic byl oproti očekávání minimální a došlo k naplnění stanoveného klíčového výkonnostního ukazatele. Průběh nasazení byl pečlivě monitorován porovnáváním dat mezi SCCM, ESET Protect a management konzolí SentinelOne. Tento jednoduchý přístup poskytl komplexní přehled o stavu nasazení v rámci Společnosti.

Bezpečnostní politika EDR byla od samého začátku nakonfigurována na "režim ochrany", který aktivně blokoval jak škodlivé, tak i podezřelé soubory. Tento přísný režim byl následně na základě zpětné vazby od uživatelů zdokonalen, přičemž úpravy zahrnovaly přidání několika málo výjimek, aby se vyvážila bezpečnost s provozní funkčností. Nutnost minimálních zásahů v bezpečnostní politice reflektuje vysokou úroveň sofistikovanosti vybraného EDR řešení.

4.3.2 **Nasazení EDR na servery**

Během fáze nasazení SentinelOne EDR na stanice uživatelů započaly kroky k nasazení také na servery. Proces nasazení byl pečlivě naplánován a proveden ve fázích, aby se minimalizovalo narušení a optimalizovala konfigurace řešení EDR pro různé role serverů. Nejprve byly bezpečnostní politiky pro servery nastaveny pouze na režim detekce. To umožnilo týmům IT a Bezpečnosti sledovat chování EDR v produkčním prostředí bez provádění automatických nápravných opatření. Režim detekce je nezbytný pro identifikaci potenciálních hrozeb a pochopení běžného provozu systému, aby bylo možné doladit nastavení EDR. Toto nastavení umožňuje ručně zasahovat při řešení výstrah, čímž se zajistí, že nedojde k neúmyslnému narušení legitimních činností systému. Postupné nasazování začalo u serverů, u nichž se předpokládalo, že instalace EDR bude mít minimální nebo žádný dopad, například u file serverů. Účelem tohoto opatrného opatření bylo snížit případná rizika spojená s implementací nového bezpečnostního softwaru na důležitých systémech. Použití serverů s malým dopadem v první fázi poskytlo cenné informace o výkonu EDR a umožnilo provést nezbytné úpravy před širším nasazením. Při nasazování řešení EDR na Citrix servery

se však objevily problémy, které poukazují na složitost implementace takových řešení v různorodých serverových prostředích. Po nasazení se na těchto serverech objevily problémy s výkonem, což si vyžádalo vytvoření specializované politiky a několik konzultací s Dodavatelem, aby se věc vyřešila. Tato situace podtrhuje význam flexibility a úzké spolupráce s dodavateli při nasazování komplexních řešení kybernetické bezpečnosti.

Přibližně deset webových aplikačních serverů integrovalo funkcionalitu skenování z příkazového řádku produktu ESET Server Security for Linux pro kontrolu nahrávaných souborů, což představovalo významnou překážku. Aby bylo možné zachovat stávající bezpečnostní funkcionalitu a zároveň začlenit SentinelOne EDR, které tuto funkci postrádá, bylo rozhodnuto o zachování řešení ESET pro jeho kritické funkce a pořízení prodloužení jeho licence na těchto serverech. Kromě toho byl SentinelOne nasazen s vlastní politikou, která vyloučila adresáře ESET a adresáře pro nahrávání souborů z rozsahu monitorování. Následná fáze nasazení musela být odložena kvůli modernizaci datových center, což poukazuje na vzájemnou závislost mezi infrastrukturními projekty a iniciativami v oblasti kybernetické bezpečnosti. Rozhodnutí nasadit SentinelOne na servery až po jejich migraci do nových datových center bylo strategické. Bylo tak učiněno proto, aby se využily lepší možnosti infrastruktury a zároveň byl zajištěn optimální výkon EDR. Během nasazení prokázalo řešení SentinelOne EDR svou robustnost a přizpůsobivost, protože si dokázalo poradit se začleněním databázových serverů a řadičů domény s novými politikami.

Vyspělost řešení byla evidentní, jelikož během tohoto nasazení nebylo nutné provádět žádné další úpravy. Významným milníkem byl závěrečný krok k dosažení téměř úplného pokrytí řešením SentinelOne v režimu ochrany, který umožňuje automatickou karanténu hrozeb. Společnost provedla tento přechod po období zpoždění způsobeném migrací datových center. To svědčí o jejich odhodlání udržovat silnou bezpečnostní pozici navzdory všem logistickým výzvám. Volba SentinelOne jako vyspělého a spolehlivého řešení EDR byla potvrzena dosažením 99% pokrytí serverů plnou ochranou a pozorováním minimálního dopadu na výkon a výskyt "false positive" hlášení.

Posledním, neméně důležitým krokem v rámci implementace bylo napojení konzole pro správu SentinelOne na stávající SIEM Společnosti, správné nastavení parsování událostí a korelačních pravidel. To proběhlo díky spolupráci s Dodavatelem řešení bez problémů.

5 Výsledky a diskuse

V této kapitole je porovnáno nasazení EDR řešení v reálném korporátním prostředí s best practice a diskusi.

Porovnáním procesů výběru a nasazení EDR řešení v reálném korporátním prostředí Společnosti, jak je popsáno v praktické části této práce, s osvědčenými postupy v oboru, bylo zjištěno vzájemné sladění, což poukazuje na úspěšnost a efektivitu obou fází výběru a nasazení, které Společnost provedla. Při bližším zkoumání je však zřejmé, že existují oblasti, kde by bylo možné dodržování osvědčených postupů zlepšit. To by mohlo vést k ještě většímu zefektivnění aktivit a zamezení konkrétních přehmatů.

Jednou z pozoruhodných odchylek od osvědčených postupů bylo neúplné určení všech technických požadavků. Společnost úspěšně nastínila své potřeby s výjimkou kritické funkce: skenování iniciované příkazovým řádkem, které pro plnou funkčnost vyžaduje deset webových aplikačních serverů. Toto opomenutí zdůrazňuje důležitost komplexních plánovacích procesů. Zapojení zástupců různých oddělení během procesu definování technických požadavků mohlo ovlivnit výsledek výběrového řízení. Jejich účast by pravděpodobně odhalila specifické potřeby, na příklad požadavek na skenování iniciované příkazovou řádkou, který byl zpočátku přehlédnut. Ve fázích plánování je klíčový meziútvarový přístup. Vlastníci a manažeři aplikací by mohli poskytnout cenné poznatky o této funkci.

Rozhodnutí vyloučit z výběru EDR modul stávajícího bezpečnostního řešení bylo založeno na jeho nízkém umístění v hodnocení společnosti Gartner a na problémech s dodavatelem stávajícího bezpečnostního řešení. Zahrnutí tohoto modulu EDR do výběrového řízení mohlo zjednodušit fázi implementace, zejména na pracovních stanicích, tím, že by se využila stávající technologie a vyžadovalo by to pouze úpravy nastavení agenta, nikoli kompletní zavedení nového řešení.

V průběhu PoC se SentinelOne odlišil od Trend Micro díky snadnějšímu nasazení a správě, lepším schopnostem detekce a účinnějším mechanismům reakce. Tyto faktory byly klíčové pro výběr společnosti SentinelOne a prokázaly hodnotu komplexního hodnocení PoC při identifikaci řešení, která nejlépe vyhovují potřebám organizace.

Zapojení dalších IT oddělení od počátku projektu mohlo zabránit případným zpožděním nebo problémům. Toho bylo možné dosáhnout sladěním harmonogramu nasazení serverů s harmonogramem migrace datových center. Tato zkušenost poukázala na důležitost

zapojení vedoucích oddělení do komunikace o projektech, které se týkají jejich oblastí, což podpoří spolupráci a informovanost v rámci projektu.

Ve fázi nasazení vyžadovaly specifické skupiny serverů, jako jsou databáze a doménové řadiče, vytvoření odlišných nastavení a politik, které by odpovídaly jejich jedinečným požadavkům. Naopak na pracovních stanicích byl od počátku implementován režim Protect. U serverů se začalo s nasazením v režimu Detect only, aby bylo možné opatrně sledovat dopad a podle potřeby upravovat nastavení bez narušení klíčových služeb.

Souhrnně lze říci, že nasazení řešení SentinelOne EDR na koncová zařízení Společnosti bylo pečlivě naplánovaným procesem, který vyvážil potřebu pokročilých funkcí EDR řešení s provozní realitou různorodého prostředí. Toto nasazení poskytuje cenné poznatky o strategii kybernetické bezpečnosti, spolupráci s dodavateli a významu přizpůsobitelných zásad pro řešení jedinečných problémů při zabezpečení komplexních IT infrastruktur.

Tyto poznatky ukazují složitost implementace řešení kybernetické bezpečnosti v korporátním prostředí a význam komplexního, všezahrnujícího přístupu, který zohledňuje odlišné vlastnosti různých součástí IT infrastruktury. Poznatky získané z tohoto nasazení podtrhují výhody spolupráce mezi odděleními, pečlivého testování před nasazením a flexibility bezpečnostních politik tak, aby splňovaly specifické požadavky různých typů systémů.

6 Závěr

Cílem této práce bylo popsání současné situace v kybernetické bezpečnosti a nejčastějších hrozeb, kterým firmy čelí, jak je možné se proti těmto hrozbám bránit pomocí antivirových, EDR a XDR řešení, porovnání těchto řešení a popsání best practice pro výběr a nasazení tohoto řešení. V praktické části popsání reálného výběru a nasazení EDR řešení v korporátním prostředí a porovnání s best practice.

V teoretické části byla nejprve popsána současná situace v kybernetické bezpečnosti spolu s pěti nejčastějšími hrozbami, kterým firmy čelí. Dále bylo popsáno fungování antivirových, Endpoint Detection and Response a eXtended Detection Response řešení. Tato řešení byla mezi sebou porovnána, stejně tak jako možnosti těchto řešení chránit společnosti před nejčastějšími hrozbami. V poslední části teoretické práce byly popsány best practice pro výběr a nasazení EDR řešení a zasazení tohoto řešení v modelu Defence in Depth, včetně vrstev toho modelu.

V praktické části byl popsán celý průběh výběrového řešení od stanovení technických požadavků, přes jednotlivá kola až po konečné rozhodnutí. Následně byl popsán průběh nasazení vybraného EDR řešení v prostředí Společnosti.

Průběh výběru a nasazení byl nakonec porovnán s best practice a výsledek ukázal úspěšnou implementaci vybraného EDR řešení i přes drobná pochybení a problémy. Nelze opomenout, že best practice jsou osvědčené postupy, které však nemusí plně vyhovovat všem firmám a společnostem, vzhledem k rozdílným velikostem, odborným znalostem odpovědných zaměstnanců, ale i finančním možnostem. Kybernetické hrozby a obrana proti nim se neustále vyvíjejí a je pro firmy všech velikostí je nutné se této oblasti věnovat.

7 Seznam použitých zdrojů

Aarness, A., 2023a. *EDR VS NGAV WHAT IS THE DIFFERENCE?.* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-ngav/
[Přístup získán 02. 02. 2024].
Aarness, A., 2023b. *NEXT-GENERATION ANTIVIRUS (NGAV).* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/
[Přístup získán 01. 02. 2024].
Aarness, A., 2023c. *WHAT IS ENDPOINT DETECTION AND RESPONSE (EDR)?.* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/
[Přístup získán 02. 02. 2024].
Aarness, A., 2023d. *WHAT IS XDR?.* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/
[Přístup získán 03. 02. 2024].
Amante, A., 2022. *Italy set to curb use of Russian anti-virus software in public sector.* [Online]
Dostupné z: https://www.reuters.com/technology/italy-set-curb-use-russian-anti-virus-software-public-sector-2022-03-17/
[Přístup získán 03. 01. 2024].
Baker, K., 2023. *WHAT IS RANSOMWARE?.* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/
[Přístup získán 05. 01. 2024].
BasuMallick, C., 2022. *What Is Endpoint Detection and Response? Definition, Importance, Key Components, and Best Practices.* [Online]
Dostupné z: https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-edr/amp/
[Přístup získán 02. 02. 2024].
BDO Digital, 2022. *Top 10 Cybersecurity Threats to Businesses in 2023.* [Online]
Dostupné z: https://www.bdodigital.com/insights/cybersecurity/top-10-cybersecurity-threats-to-businesses-in-2023
[Přístup získán 04. 01. 2024].
Capterra, 2024. *Endpoint Detection and Response Software Buyers Guide.* [Online]
Dostupné z: https://www.capterra.com/endpoint-detection-and-response-software/buyers-guide/
[Přístup získán 04. 02. 2024].
Caufield, M., 2023. *ChatGPT is changing the phishing game.* [Online]
Dostupné z: https://www.securityinfowatch.com/cybersecurity/information-security/breach-detection/article/53057705/chatgpt-is-changing-the-phishing-game
[Přístup získán 06. 01. 2024].
CrowdStrike, 2022. *Exploit kits.* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/attack-types/exploit-kits/
[Přístup získán 04 01 2024].
CYNET, 2024. *EDR vs Antivirus: What Is the Difference?.* [Online]
Dostupné z: https://www.cynet.com/endpoint-protection-and-edr/edr-vs-antivirus/#
[Přístup získán 02. 02. 2024].

Česká spořitelna, 2019. *Česká spořitelna varuje před podvodníky, zasílají jejím jménem podvodné SMS.* [Online]
Dostupné z: https://www.mesec.cz/aktuality/ceska-sporitelna-varuje-pred-podvodniky-zasilaji-jejim-jmenem-podvodne-sms/
[Přístup získán 06. 01. 2024].
Das, R., 2021. *Deploying Endpoint Detection & Response: 5 Best Practices.* [Online]
Dostupné z: https://platform.keesingtechnologies.com/deploying-endpoint-detection-response-5-best-practices/
[Přístup získán 04. 02. 2024].
ESET, 2023a. *ESET Endpoint Security.* [Online]
Dostupné z: https://www.eset.com/fileadmin/ESET/CZ/Produktove_listy/firmy/EndpointSolutions/ESET_Endpoint_Security_overview_cs-CZ.pdf
[Přístup získán 08. 02. 2024].
ESET, 2023b. *Eset Protect Demo.* [Online]
Dostupné z: https://www.eset.com/cz/firmy/demo/
[Přístup získán 08. 02. 2024].
ESET, 2023c. *ESET Server Security for Linux.* [Online]
Dostupné z: https://help.eset.com/essl/10.2/en-US/key_features_of_the_system.html
[Přístup získán 08. 02. 2024].
ESET, 2023d. *ESET Server Security for Microsoft Windows Server.* [Online]
Dostupné z: https://help.eset.com/efsw/10.0/en-US/key_features.html
[Přístup získán 08. 02. 2024].
ESET, 2024a. *ESET Protect Demo.* [Online]
Dostupné z: https://www.eset.com/int/business/demo/
[Přístup získán 18. 02. 2024].
ESET, 2024b. *What is the difference between a Virus Signature Database update and a Program Component Update (PCU)?.* [Online]
Dostupné z: https://eset.version-2.sg/html/326/817
[Přístup získán 01. 02. 2024].
ESET, 2024c. *ESET Endpoint Security Protection Status.* [Online]
Dostupné z: https://help.eset.com/ees/11/en-US/?idh_page_protection_status.html=
[Přístup získán 01. 02. 2024].
European Commision, 2023. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* [Online]
Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[Přístup získán 04. 01. 2024].
Firstbrook, P. & Lawson, C., 2021. *Innovation Insight for Extended Detection and Response.* [Online]
Dostupné z: https://www.gartner.com/document/3982247
[Přístup získán 03. 02. 2024].
Fortinet, 2024. *What Is a Zero Day Attack?.* [Online]
Dostupné z: https://www.fortinet.com/resources/cyberglossary/zero-day-attack
[Přístup získán 08 01 2024].
GEORGE, A. S., GEORGE, A. S. H., BASKAR, T. & PANDEY, D., 2021. *XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future,* místo neznámé: autor neznámý

Ghost, 2023. *What is Defense in Depth.* [Online]
Dostupné z: https://medium.com/@cyber.ghost/what-is-defense-in-depth-5a8596839f65
[Přístup získán 04. 02. 2024].
Haas, T. P., 2022. *Log4J shows: Dangerous Supply chain attacks are becoming increasingly popular with attackers.* [Online]
Dostupné z: https://www.itsa365.de/en/news-knowledge/2022/interview/log4j-shows-dangerous-supply-chain-attacks-are-becoming-increasingly-popular-with-attackers
[Přístup získán 06. 01. 2024].
Hand, M., 2023. *Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems.* místo neznámé:No Starch Press.
Huntley, S., 2023. *Fog of war: how the Ukraine conflict transformed the cyber threat landscape.* [Online]
Dostupné z: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
[Přístup získán 02. 01. 2024].
Check Point Research Team, 2021. *The Numbers Behind Log4j Vulnerability CVE-2021-44228.* [Online]
Dostupné z: https://blog.checkpoint.com/security/the-numbers-behind-a-cyber-pandemic-detailed-dive/
[Přístup získán 07. 01. 2024].
Chuvakin, A., 2013. *Named Endpoint Threat Detection Response.* [Online]
Dostupné z: https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/
[Přístup získán 01. 02. 2024].
IBM, 2023a. *What is ransomware?.* [Online]
Dostupné z: https://www.ibm.com/topics/ransomware
[Přístup získán 05. 01. 2024].
IBM, 2023b. *What is the Log4j vulnerability?.* [Online]
Dostupné z: https://www.ibm.com/topics/log4j
[Přístup získán 07. 01. 2024].
Info Exchange, 2022. *Signature-Based Vs Behavior-Based Cybersecurity.* [Online]
Dostupné z: https://www.infoexchangeja.com/blog/data-security/the-difference-between-signature-based-and-behavior-based-detection/
[Přístup získán 01. 02. 2024].
It, R., 2024. *The Story of Creeper vs Reaper – The First Virus and Anti-Virus Programs.* [Online]
Dostupné z: https://theassistant.io/business/the-story-of-creeper-vs-reaper-the-first-virus-and-anti-virus-programs/
[Přístup získán 10. 01. 2024].
Kayiş, H., 2019. *EDR (Endpoint Detection and Response).* [Online]
Dostupné z: https://medium.com/@hakankayis/edr-endpoint-detection-and-response-3ad5218c1515
[Přístup získán 02. 02. 2024].
Landesman, M., 2019. *What Is a Virus Signature?.* [Online]
Dostupné z: https://www.lifewire.com/what-is-a-virus-signature-153629
[Přístup získán 01. 02. 2024].
Lau, J., 2023. *State of Cybersecurity 2023: Navigating Current and Emerging Threats.* [Online]
Dostupné z: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/state-

of-cybersecurity-2023-navigating-current-and-emerging-threats
[Přístup získán 04. 01. 2024].
Lau, J., 2023. *State of Cybersecurity 2023: Navigating Current and Emerging Threats.* [Online]
Dostupné z: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/state-of-cybersecurity-2023-navigating-current-and-emerging-threats
[Přístup získán 04. 01. 2024].
Lenaerts-Bergmans, B., 2022. *SPEAR PHISHING VS PHISHING.* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing-vs-phishing/
[Přístup získán 06. 01. 2024].
Lenaerts-Bergmans, B., 2023. *WHAT IS A SUPPLY CHAIN ATTACK?.* [Online]
Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/
McKinsey & Company, 2022. *Cybersecurity trends: Looking over the horizon.* [Online]
Dostupné z: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon
[Přístup získán 03. 01. 2024].
Merriam-Webster, 2024. *best practice.* [Online]
Dostupné z: https://www.merriam-webster.com/dictionary/best%20practice#:~:text=%3A%20a%20procedure%20that%20has%20been,standard%20suitable%20for%20widespread%20adoption
[Přístup získán 01. 02. 2024].
Microsoft Defender Security Research Team, 2017. *WannaCrypt ransomware worm targets out-of-date systems.* [Online]
Dostupné z: https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
[Přístup získán 05. 01. 2024].
Mishra, A., 2022. *Modern Cybersecurity Strategies for Enterprises.* místo neznámé:BPB Publications.
Mughal, A. A., 2023. *The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection.* [Online]
Dostupné z: https://research.tensorgate.org/index.php/IJIAC/article/view/19/18
[Přístup získán 04. 02. 2024].
NÚKIB, 2022. *Ruské firmy a dopady na ICT.* [Online]
Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1820-ruske-firmy-a-dopady-na-ict/
[Přístup získán 03. 01. 2024].
NUKIB, 2023. *Ransomware: Doporučení pro mitigaci, prevenci a reakci.* [Online]
Dostupné z: https://www.nukib.cz/download/publikace/navody/RANSOMWARE%20-%20Doporuceni%20pro%20mitigaci%20prevenci%20a%20reakci.pdf
[Přístup získán 05. 01. 2024].
Ozkaya, D. E. & Diogenes, Y., 2019. *Cybersecurity – Attack and Defense Strategies - Second Edition.* místo neznámé:Packt Publishing.
Pipikate, A., Barrachin, M. & Crawford, S., 2021. *These are the top cybersecurity challenges of 2021.* [Online]
Dostupné z: https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/
[Přístup získán 03. 01. 2024].

Rains, T., 2020. *Cybersecurity Threats, Malware Trends, and Strategies.* místo neznámé:Packt Publishing.
Sahay, M., 2024. *Who Invented the Antivirus? A History of Antivirus Software..* [Online]
Dostupné z: https://www.thepcinsider.com/who-invented-antivirus-history-timeline-evolution/
[Přístup získán 01. 02. 2024].
SentinelOne, 2019. *SentinelOne.* [Online]
Dostupné z: https://twitter.com/SentinelOne/status/1123373244566818816/photo/1
SentinelOne, 2023. *Endpoint, Identity and Cloud | Top Cyber Attacks of 2023 (So Far).* [Online]
Dostupné z: https://www.sentinelone.com/blog/endpoint-identity-and-cloud-top-cyber-attacks-of-2023-so-far/
[Přístup získán 09. 01. 2024].
SentinelOne, 2024. *What Is Extended Detection And Response (XDR)?.* [Online]
Dostupné z: https://www.sentinelone.com/cybersecurity-101/extended-detection-response-xdr/
[Přístup získán 03. 02. 2024].
Stephenson, B., 2020. *What Is a Computer Virus?.* [Online]
Dostupné z: https://www.lifewire.com/what-is-a-computer-virus-4799053
Szor, P., 2005. *The Art of Computer Virus Research and Defense.* místo neznámé:Addison-Wesley Professional.
Šmerek, M., 2014. *Moodle Univerzita Obrany.* [Online]
Dostupné z:
https://moodle.unob.cz/pluginfile.php/35526/mod_resource/content/2/OV_T13.pdf
[Přístup získán 09. 02. 2024].
The White House, 2023. *International Counter Ransomware Initiative 2023 Joint Statement.* [Online]
Dostupné z: https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/
[Přístup získán 05. 01. 2024].
Tiel, B. v., 2023. *New European NIS2 directive: stricter requirements for cyber security.* [Online]
Dostupné z: https://www.pwc.nl/en/insights-and-publications/themes/risk-regulation/new-european-nis2-directive-stricter-requirements-for-cyber-security.html
[Přístup získán 04. 01. 2024].
Torres, G., 2017. *What Is a Computer Virus?.* [Online]
Dostupné z: https://www.avg.com/en/signal/what-is-a-computer-virus
[Přístup získán 04. 01. 2024].
Trellix, 2024. *What Is Endpoint Detection and Response?.* [Online]
Dostupné z: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-detection-and-response/
[Přístup získán 02. 02. 2024].
Trio Team, 2024. *6 Steps to Integrating EDR in Your IT Department.* [Online]
Dostupné z: https://www.trio.so/blog/endpoint-detection-and-response/
[Přístup získán 04. 02. 2024].
Vlastní zpracování, 2022. *Průběh výběrového řízení.* místo neznámé:Společnost.
Vlastní zpracování, 2024. místo neznámé: autor neznámý

Yehushua, N. & Kosayev, U., 2021. *Antivirus Bypass Techniques: Learn practical techniques and tactics to combat, bypass, and evade antivirus software.* místo neznámé:Packt Publishing.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

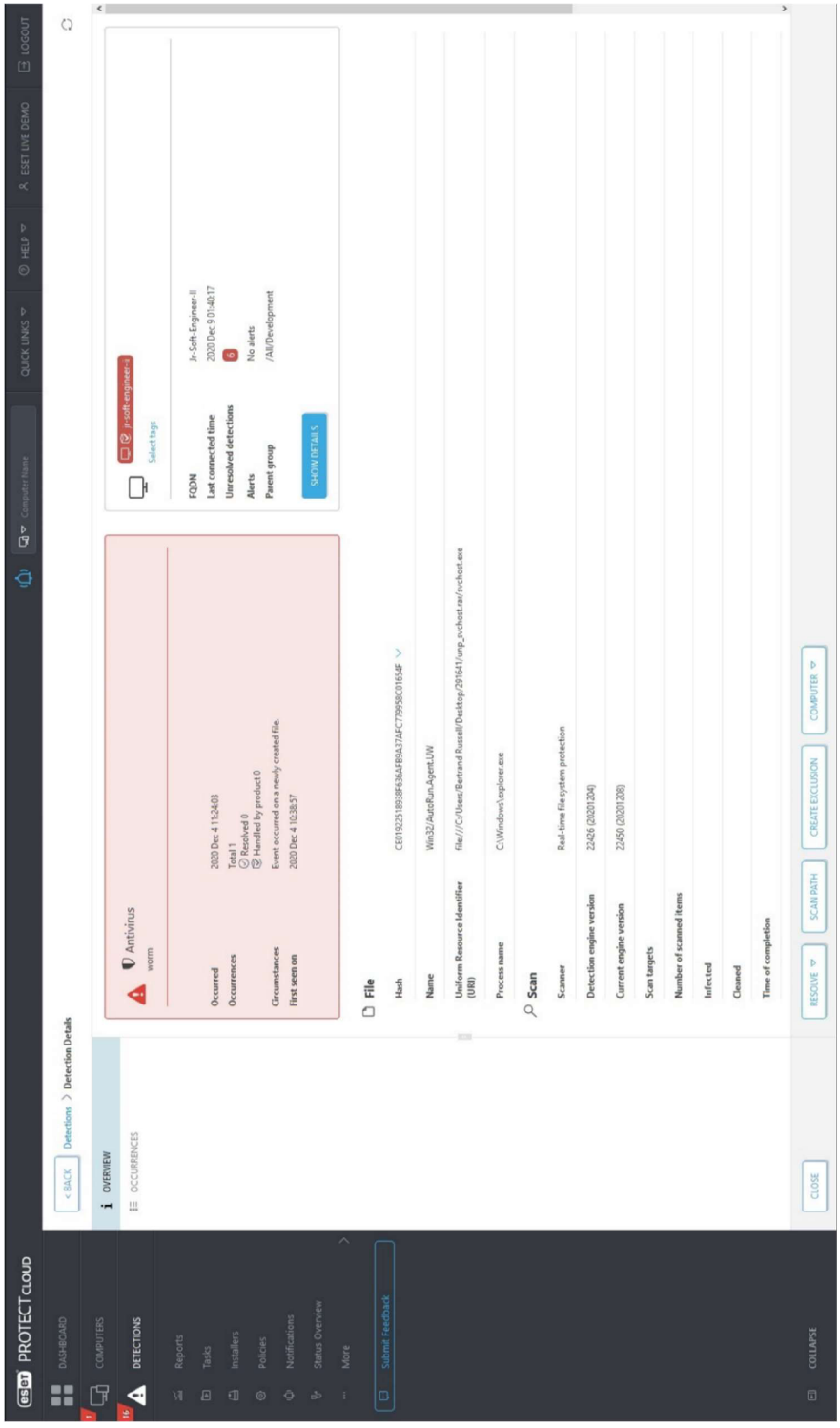
8.2 Seznam tabulek

8.3 Seznam použitých zkratek

CVSS – Common Vulnerability Scoring Systém
DLP – Data Loss Prevention
DMZ – Demilitarized Zone
GDPR – General Data Protection Regulation
IoC – Indicators of Compromise
ISACA – Information Systems Audit and Control Association
MBR – Master Boot Record
MFA - Multi Factor Authentication
MSI – Microsoft Installer
RBAC – Role Based Access Control
RDP – Remote Desktop Protocol
SCCM – System Center Configuration Manager
SIEM – Security Information and Event Management
WAF – Web Application Firewall

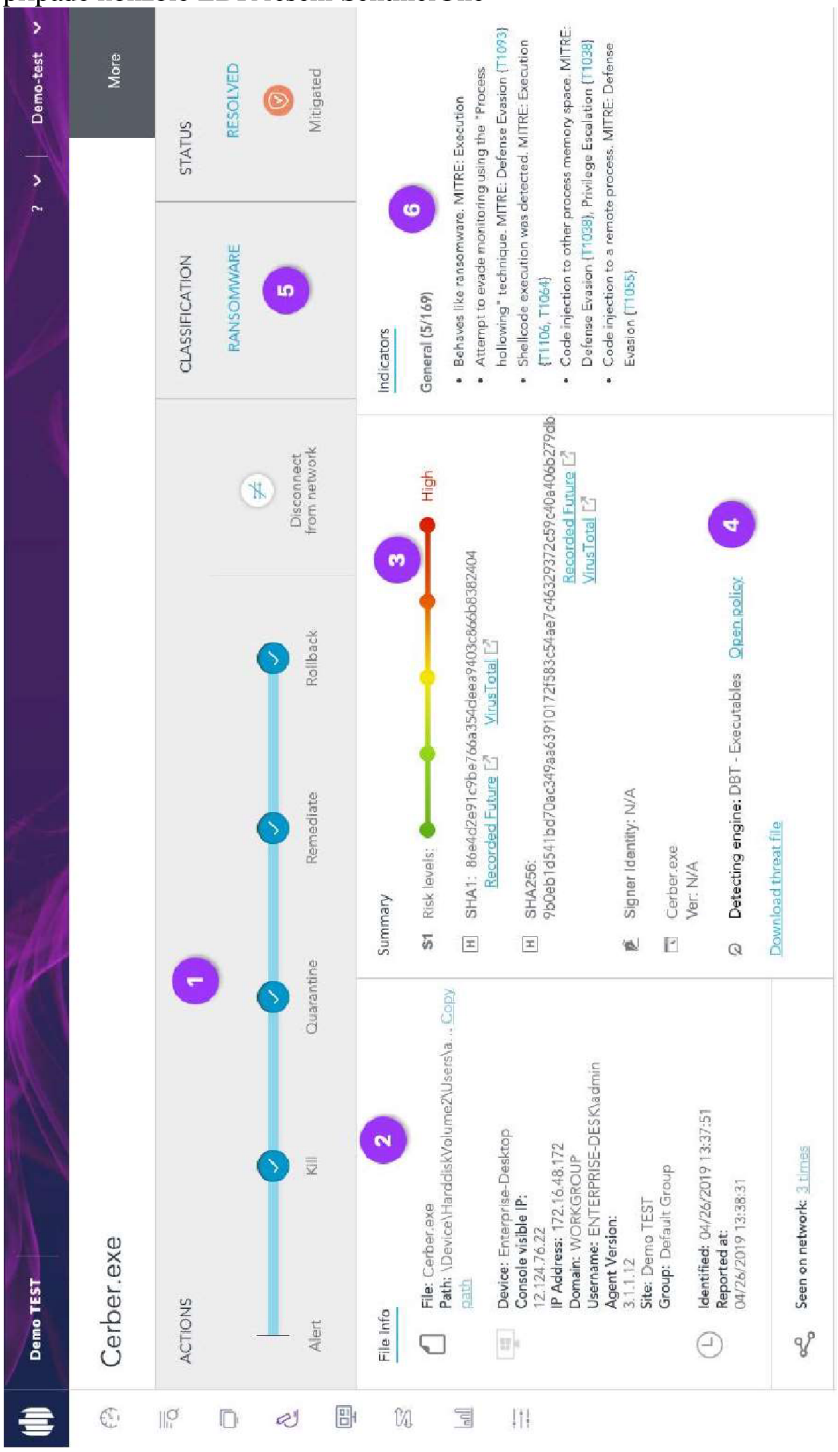
Přílohy

Příloha 1 Obrázek 5 Informace k nalezenému malware v tradičním antiviru, v tomto případě konzole ESET Protect



Zdroj: (ESET, 2024a)

Příloha 2 Obrázek 6 Informace k nalezenému a odstraněnému malware v EDR, v tomto případě konzole EDR řešení SentinelOne



Zdroj: (SentinelOne, 2019)

Příloha 3 Tabulka 10 Tabulka porovnání cenových nabídek po prvním kole

	Uchazeč 1 SaaS - roční předplatba	Uchazeč 2 SaaS - roční platba za lic.	Uchazeč 3 SaaS - roční předplatba	Uchazeč 4 SaaS - roční předplatba	Uchazeč 5 SaaS - roční předplatba	Uchazeč 6 SaaS - roční předplatba	Uchazeč 7 SaaS - roční předplatba	Uchazeč 8 SaaS - roční předplatba
Řešení	**SentinelOne**	**Palo Alto Cortex XDR**	**Trend Micro**	**SentinelOne**	**Bitdefender**	**Bitdefender**	**Microsoft**	**CheckPoint**
	cena v Kč vč. DPH	cena v Kč vč. DPH	cena v Kč vč. DPH	cena v Kč vč. DPH	cena v Kč vč. DPH	cena v Kč vč. DPH	cena v Kč vč. DPH	cena v Kč vč. DPH
Licence Endpoint (6400ks)	3 981 633,26 Kč	12 611 796,66 Kč	8 944 971,27 Kč	4 130 745,19 Kč	6 776 484,00 Kč	7 314 450,00 Kč	5 771 525,76 Kč	3 467 695,44 Kč
Licence Server (1400ks)	1 288 960,37 Kč			1 338 005,90 Kč				
Jiné (7800ks)	1 371 235,00 Kč			1 421 164,36 Kč				3 116 805,12 Kč
Implementace	460 405,00 Kč	1 782 120,00 Kč	387 200,00 Kč	130 680,00 Kč	470 932,00 Kč	454 960,00 Kč	3 085 790,40 Kč	290 400,00 Kč
Servisní podpora - 1 rok	798 600,00 Kč	387 684,00 Kč	464 640,00 Kč	- Kč	201 828,00 Kč	261 360,00 Kč	634 669,20 Kč	360 096,00 Kč
Celkem za 1. rok	**7 900 833,62 Kč**	**14 781 600,66 Kč**	**9 796 811,27 Kč**	**7 020 595,45 Kč**	**7 449 244,00 Kč**	**8 030 770,00 Kč**	**9 491 985,36 Kč**	**7 234 996,56 Kč**
Celkem za 3 roky	**22 781 690,87 Kč**	**26 079 563,40 Kč**	**28 616 033,80 Kč**	**20 800 426,35 Kč**	**21 405 868,00 Kč**	**23 182 390,00 Kč**	**22 304 375,28 Kč**	**20 961 565,68 Kč**

Zdroj: (Vlastní zpracování, 2022)

Příloha 4 Tabulka 11 Hodnotící matice technických požadavků po workshopech

Položka hodnocení	Váha	Uchazeč 8 / Check Point		Uchazeč 5 / Bitdefender		Uchazeč 3 / Trend Micro		Ucahzeč 7 / Microsoft		Uchazeč 1 / Sentinel One		Uchazeč 2 / Palo Alto Networks		Maximální možné ohodnocení	
Vysoká spolehlivost detekce relevantních událostí (bude hodnoceno na základě výsledků dané technologie v testu MITRE 2021 Carbanak+FIN7 ATT&CK Evaluation).	**3**	2	**6**	2	**6**	3	**9**	2	**6**	3	**9**	3	**9**	3	**9**
Jednotná centrální konzole pro řešení bezpečnostních incidentů, s minimalizovanou potřebou pro přecházení mezi komponenty/prostředími řešení.	**3**	2	**6**	2	**6**	2	**6**	1	**3**	3	**9**	2	**6**	3	**9**
Integrace modelu MITRE ATT&CK v rámci systému řešení incidentů, včetně automatizovaného real-time mapování událostí dle daného modelu.	1	3	**3**	2	**2**	3	**3**	2	**2**	3	**3**	3	**3**	3	**3**
Přehledná vizualizace probíhajícího incidentu v rámci centrální konzole.	2	1	**2**	2	**4**	3	**6**	2	**4**	3	**6**	1	**2**	3	**6**
Široké spektrum užívaných senzorů/zdrojů událostí/telemetrie (včetně např. síťové sondy).	2	0	**0**	2	**4**	2	**4**	1	**2**	1	**2**	1	**2**	3	**6**
Široké spektrum možností reakce na probíhající incident na stanicích/serverech s agentem.	3	1	**3**	2	**6**	3	**9**	2	**6**	3	**9**	3	**9**	3	**9**
Možnost retence dat minimálně 3 měsíce, preferovaně až 12 měsíců.	2	2	**4**	1	**2**	2	**4**	1	**2**	2	**4**	2	**4**	3	**6**
Detekce zranitelností na stanicích/serverech s agentem.	1	2	**2**	2	**2**	3	**3**	1	**1**	1	**1**	2	**2**	3	**3**
Možnost Device Control pro management užívání externích médií na stanicích.	1	3	**3**	1	**1**	2	**2**	0	**0**	2	**2**	1	**1**	3	**3**
Sandbox funkcionalita pro automatizovanou analýzu detekovaných vzorků.	2	1	**2**	2	**4**	2	**4**	1	**2**	0	**0**	2	**4**	3	**6**
Přehledné mapování spuštěných procesu v rámci vyšetřování bezpečnostního incidentu.	1	1	**1**	2	**2**	2	**2**	2	**2**	2	**2**	2	**2**	3	**3**
Možnost napojení externích zdrojů Threat Intelligence.	2	0	**0**	0	**0**	3	**6**	0	**0**	1	**2**	2	**4**	3	**6**
Možnost vytváření vlastních (custom) pravidel pro vyhledávání IoC.	2	2	**4**	2	**4**	2	**4**	2	**4**	1	**2**	2	**4**	3	**6**
Možnosti ochrany zranitelných verzí OS/aplikací např. virtual patchingem nebo jiným způsobem.	1	1	**1**	0	**0**	3	**3**	1	**1**	1	**1**	2	**2**	3	**3**
Výsledky demonstrací a ukázek jednotlivých zadaných use cases během workshopu	5	2	**10**	1	**5**	2	**10**	2	**10**	2	**10**	2	**10**	3	**15**
Kvalita přípravy nabídky a workshopu	1	2	**2**	1	**1**	3	**3**	2	**2**	2	**2**	2	**2**	3	**3**
Preference budoucích operátorů	1	3	**3**	1	**1**	2	**2**	1	**1**	3	**3**	2	**2**	3	**3**
			52		**50**		**80**		**48**		**67**		**68**		**99**
Procentuální hodnocení z maximálního možného počtu bodů			**52,5%**		**50,5%**		**80,8%**		**48,5%**		**67,7%**		**68,7%**		

Zdroj: (Vlastní zpracování, 2022)