LEXNOVA

Smlouva o poskytování expertních služeb a dalších odborných služeb kybernetické bezpečnosti

(dále jen „Smlouva")

uzavřená v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ") za přiměřeného použití ustanovení § 2586 a násl. téhož zákona.

Smlouva č.: 2026/CRM_344

Smluvní strany

Název:	**Lexnova Technology s.r.o.**
Spisová značka:	C 414872 vedená u Městského soudu v Praze
Sídlo:	Na rovnosti 2274/12, Žižkov, 130 00 Praha 3
IČO:	22340564
Zastoupena:	Miroslav Kvapil, MSc., jednatelem
(dále jen „**Poskytovatel**")	

a

Název:	**Domov pro seniory Kociánka, příspěvková organizace**
Sídlo:	Kociánka 1/8, 612 00 Brno
IČ:	70887284
Zastoupena:	
(dále jen „**Objednatel**")	Ing. Naděžda Křemečková, ředitelka

(Poskytovatel a Objednatel dále též společně jako „**Smluvní strany**" se dohodli na následujícím:

1. Předmět smlouvy

1.1 Předmětem této Smlouvy je využití zdrojů, know-how a organizačních schopností Poskytovatele k provádění odborných expertních činností v oblasti kybernetické bezpečnosti dle Specifikace Expertních služeb kybernetické bezpečnosti, která tvoří Přílohu č. 1 této Smlouvy (dále jen „Expertní služby") a dalších odborných služeb kybernetické bezpečnosti, které jsou uvedeny v Příloze č. 2 této Smlouvy. Expertní služby budou poskytovány v souladu se zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, v platném znění (dále jen „ZoKB"), a souvisejícími prováděcími právními předpisy, zejména vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (vyhláška o kybernetické bezpečnosti), a vyhláškou č. 408/2025 Sb., o regulovaných službách, v platném znění, a směřují k naplnění povinností Objednatele jako poskytovatele regulované služby podle uvedené právní úpravy. Předmětem Smlouvy je závazek Poskytovatele poskytovat Objednateli Expertní služby v souladu se všemi relevantními závaznými právními předpisy, či příslušnými technickými normami, které se k danému plnění vztahují, jakož i se Smlouvou sjednanými podmínkami, a současně závazek Objednatele zaplatit Poskytovateli cenu stanovenou v čl. 3. Smlouvy za jejich řádné poskytnutí.

1.2 Poskytováním Expertních služeb se rozumí veškerá činnost Poskytovatele dle Smlouvy směřující k provádění činností v rozsahu dle Přílohy č. 1 – Specifikace Expertních služeb kybernetické bezpečnosti.

1.3 Poskytovatel se zavazuje služby poskytovat prostřednictvím osoby, která splňuje požadavky Objednatele na kvalifikaci dle této Smlouvy.

2. Lhůta, způsob a místo plnění

2.1 Plnění předmětu smlouvy bude zahájeno dnem účinnosti této smlouvy.

2.2 Místem plnění jsou prostory Poskytovatele formou vzdálené podpory, případně prostory Objednatele.

3. Cena a platební podmínky

3.1 Za řádné poskytnutí Expertních služeb dle Přílohy č. 1 této Smlouvy v objemu 24 člověkohodin měsíčně a za odborné služby uvedení v Příloze č. 2 této smlouvy se smluvní strany dohodly na paušální sazbě ve výši 49 000 Kč (Poskytovatel není plátcem DPH). V případě překročení časové alokace uvedené v Příloze č. 1 bude Poskytovatelem nad rámec této paušální sazby fakturována hodinová sazba ve výši 1 500 Kč. Jakékoliv překročení časové alokace a s tím spojené fakturace podléhá předchozímu písemnému schválení Objednatelem.

Paušální sazba za Expertní služby	
Cena bez DPH za měsíc:	49 000 Kč (Poskytovatel není plátcem DPH)
Hodinová sazba Expertních služeb	
Cena bez DPH za 1 člověkohodinu	1 500 Kč (Poskytovatel není plátcem DPH)

3.2 Součástí fakturace bude soupis realizovaných prací za fakturované období.

3.3 Smluvní strany si sjednaly, že Objednatel bude hradit Poskytovateli odměnu za Expertní služby vždy na měsíční bázi, a to bezhotovostním převodem na bankovní účet uvedený na příslušné faktuře se splatností 14 dnů.

3.4 Při prodlení Objednatele s úhradou faktury se sjednává smluvní pokuta ve výši 0,05 % z dlužné částky za každý den prodlení. Smluvní pokuta je splatná do 15, slovy patnácti dní, ode dne doručení výzvy k úhradě této smluvní pokuty Objednateli Poskytovatelem.

3.5 Faktury budou Objednateli odesílány elektronicky na email: [redacted]

4. Součinnost, práva a povinnosti smluvních stran

4.1 Objednatel se zavazuje Poskytovateli poskytovat součinnost vyplývající ze Smlouvy, a to pouze v nezbytně nutném rozsahu, a nikoliv nad rámec součinnosti jinak obvyklé při poskytování obdobného druhu plnění.

4.2 Objednatel se zavazuje Poskytovateli poskytnout veškeré doklady, písemnosti, dokumentaci a informace nezbytné pro plnění předmětu Smlouvy.

4.3 Objednatel se zavazuje umožnit Poskytovateli přístup v nezbytně nutném rozsahu do objektů ve vlastnictví Objednatele a k technickým prostředkům v rozsahu Systému řízení bezpečnosti informací, je-li to nezbytné pro plnění předmětu této Smlouvy.

4.4 Objednatel je oprávněn zajistit poskytnutí součinnosti třetími osobami.

4.5 Poskytovatel je povinen postupovat při plnění předmětu Smlouvy s odbornou péčí, podle nejlepších znalostí a schopností a sledovat a chránit oprávněné zájmy Objednatele. Dále je povinen postupovat v souladu s pokyny Objednatele a jeho interními předpisy, které souvisí s předmětem plnění Smlouvy a které Objednatel Poskytovateli poskytne.

4.6 Poskytovatel se zavazuje informovat Objednatele o všech skutečnostech majících vliv na plnění této Smlouvy.

4.7 Poskytovatel je povinen v průběhu poskytování Expertních služeb neprodleně upozornit Objednatele na nevhodnost jeho pokynů nebo předané dokumentace. Toto upozornění musí mít písemnou formu. V takovém případě je Objednatel povinen se k tomuto upozornění bez zbytečného odkladu písemně vyjádřit a je povinen učinit veškerá opatření, aby Poskytovatel mohl pokračovat v poskytování Expertních služeb řádně a včas.

5. Zajištění důvěrnosti předávaných dat (mlčenlivost)

5.1 Poskytovatel je povinen při užívání a čerpání jakýchkoli informací, dat, podkladů, zejména o cílech a smluvním vztahu k veřejné zakázce a jejího plnění, informačních systémech, personálním zabezpečení, vnitřní struktuře organizace a o skutečnostech, které se vztahují k bezpečnostním a technickým opatřením, kdy se stává příjemcem a uživatelem těchto informací, jako chráněných informací, ve smyslu ustanovení § 1730 OZ, dodržovat zákonné předpisy pro oblast ochrany osobních údajů, kybernetické bezpečnosti, interní předpisy a počínat si při svém jednání tak, aby nedocházelo k porušování bezpečnostních opatření, nebyla snižována a poškozována bezpečnostní image Objednatele a důvěryhodnost těchto zdrojů a nedošlo k neoprávněnému zásahu do sítí a informačních systémů s následkem jejich poškození.

5.2 Poskytovatel je dle zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění, a dle Nařízení Evropského Parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, povinen zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů v informačním systému Objednatele. Povinnost mlčenlivosti trvá i po ukončení účinnosti Smlouvy. Poskytovatel odpovídá Objednateli v plné míře za škodu, kterou mu způsobí porušením tohoto ustanovení

6. Trvání smlouvy

6.1 Tato smlouva se uzavírá na dobu určitou, a to na 12 měsíců ode dne nabytí její účinnosti. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem jejího uveřejnění v registru smluv dle zákona č. 340/2015 Sb. (o registru smluv).

6.2 Výpovědní doba činí 3 měsíce a začíná běžet prvním dnem kalendářního měsíce následujícího po měsíci, v němž byla výpověď doručena druhé smluvní straně a končí uplynutím posledního dne příslušného kalendářního měsíce.

7. Odpovědnost za vady

7.1 Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a Smlouvy. Poskytovatel odpovídá za škodu rovněž v případě, že část plnění poskytuje prostřednictvím poddodavatele.

7.2 Poskytovatel odpovídá za odbornou úroveň poskytovaných Expertních služeb dle této Smlouvy. Právo na náhradu újmy vzniklé neodborným provedením poskytovaných Expertních služeb se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

7.3 V případě porušení zákona v oblasti kybernetické bezpečnosti jednáním ze strany Poskytovatele je Objednatel oprávněn požadovat finanční náhradu škody ve výši sankce za spáchání správního deliktu za každé porušení dle zákona o kybernetické bezpečnosti, která bude správním orgánem pravomocně udělena Objednateli dle příslušného zákona, maximálně však do výše odpovídající 12násobku měsíční paušální odměny dle této Smlouvy.

7.4 Žádná ze smluvních stran není odpovědná za škodu vzniklou porušením povinnosti ze Smlouvy, prokáže-li, že mu ve splnění takové povinnosti dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním smluvené povinnosti v prodlení, ani překážka, kterou byl škůdce podle smluvené povinnosti povinen překonat, ho však povinnosti k náhradě nezprostí. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé překážky bránící řádnému plnění Smlouvy a dále se zavazují k vyvinutí maximálního úsilí k jejich odvrácení a překonání.

7.5 Poskytovatel se zavazuje udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě.

8. Závěrečná ustanovení

8.1 Smlouva představuje úplnou dohodu smluvních stran o předmětu Smlouvy a všech náležitostech, které smluvní strany měly a chtěly ve Smlouvě ujednat, a které považují za důležité pro závaznost Smlouvy. Smlouvu lze měnit či doplňovat pouze písemnými dodatky odsouhlasenými oběma smluvními stranami.

8.2 Poskytovatel je tímto oprávněn uvádět název a/či logo Objednatele ve svém seznamu referenčních klientů na svých internetových prezentacích, sociálních sítích, propagačních materiálech a podobně.

8.3 Smluvní strany se podpisem Smlouvy dohodly, že vylučují aplikaci ustanovení § 557 OZ.

8.4 Po ukončení Smlouvy z jakéhokoli důvodu se Poskytovatel zavazuje bez zbytečného odkladu vrátit Objednateli (nebo prokazatelně zničit) veškeré dokumenty obsahující důvěrné informace včetně všech jejich kopií, a to včetně veškerých poznámek, na které se povinnost mlčenlivosti vztahuje.

Výjimkou jsou doklady, které umožňují Poskytovateli hájit jeho práva v případném soudním řízení ze sporů vyplývajících ze Smlouvy, které je Poskytovatel oprávněn uchovat nejdéle po dobu 4 let od ukončení Smlouvy.

8.5 Záležitosti ve Smlouvě výslovně neupravené se řídí příslušnými ustanoveními OZ a příslušnými právními předpisy souvisejícími. Veškeré případné spory ze Smlouvy budou v prvé řadě řešeny smírem (tento postup se nevztahuje na vymáhání finančních pohledávek vzniklých z porušení povinnosti zaplatit pohledávku). Pokud smíru nebude dosaženo během 30 dnů, všechny spory ze Smlouvy a v souvislosti s ní budou řešeny věcně a místně příslušným soudem v České republice.

8.6 Smlouva je vyhotovena ve dvou vyhotoveních, z nichž jedno vyhotovení obdrží Objednatel a jedno vyhotovení obdrží Poskytovatel.

8.7 Nedílnou součástí Smlouvy jsou následující přílohy:

Příloha č. 1 Specifikace Expertních služeb kybernetické bezpečnost

Příloha č. 2 Specifikace dalších odborných služeb kybernetické bezpečnost

8.8 Smluvní strany shodně prohlašují, že se seznámily s obsahem Smlouvy, který je dostatečně určitý a srozumitelný, a že se Smlouvou souhlasí v plném rozsahu. Smluvní strany uzavírají Smlouvu na základě vážné a svobodné vůle prosté omylu a na důkaz toho připojují své vlastnoruční podpisy.

V Praze, dne.....

Miroslav Kvapil

Digitálně podepsal Miroslav Kvapil
Datum: 2026.04.16 12:34:28 +02'00'

Poskytovatel
Lexnova Technology s.r.o.
Miroslav Kvapil MSc., jednatel

V Brně, dne.....

Ing. Naděžda Křemečková

Digitálně podepsal Ing. Naděžda Křemečková
Datum: 2026.04.16 13:44:51 +02'00'

Objednatel
Domov pro seniory Kociánka,
příspěvková organizace
Ing. Naděžda Křemečková, ředitelka

Příloha č. 1 – Specifikace Expertních služeb kybernetické bezpečnosti

Poskytovatel bude poskytovat pro Objednatele následující Expertní služby zahrnující zejména následující dílčí plnění

Manažer kybernetické bezpečnosti

Právní základ: § 5 odst. 1 a § 4 odst. 4 písm. a) VoKB č. 409/2025 Sb.

Manažer kybernetické bezpečnosti (dále jen „MKB") je pověřen řízením systému řízení bezpečnosti informací (ISMS) a koordinací činností souvisejících s kybernetickou bezpečností regulované služby. MKB odpovídá za řízení bezpečnostních opatření, dohled nad jejich implementací a za pravidelné informování vrcholného vedení o stavu kybernetické bezpečnosti.

MKB nesmí být pověřen výkonem rolí odpovědných za provoz technických aktiv regulované služby.

Rozsah činnosti manažera kybernetické bezpečnosti dle VoKB 409/2025:

1. Řízení systému řízení bezpečnosti informací (ISMS), včetně jeho zavedení, provozování, monitorování, přezkoumání a zlepšování (§ 5 odst. 1 písm. a) ve vazbě na § 3).
2. Koordinace zavádění a provozu bezpečnostních opatření vyplývajících ze zákona č. 264/2025 Sb. a VoKB 409/2025 (§ 3 písm. c).
3. Zajištění řízení rizik, včetně organizace hodnocení rizik, zpracování zprávy o hodnocení rizik a plánu zvládání rizik (§ 8 odst. 1 písm. e) a g)).
4. Pravidelné informování vrcholného vedení o stavu kybernetické bezpečnosti, rizicích, incidentech a plnění bezpečnostních opatření (§ 5 odst. 1 písm. b)).
5. Zajištění přípravy podkladů pro vrcholné vedení a výbor pro řízení kybernetické bezpečnosti, včetně zpráv o ISMS, rizicích a auditech (§ 4 odst. 2).
6. Účast na činnosti výboru pro řízení kybernetické bezpečnosti a koordinace bezpečnostních aktivit napříč organizací (§ 4 odst. 3).
7. Koordinace řešení kybernetických bezpečnostních incidentů, včetně dohledu nad procesy detekce, vyhodnocení a zvládání incidentů (§ 14).
8. Zajištění zavedení a aktualizace bezpečnostní politiky a bezpečnostní dokumentace a dohled nad jejich dodržováním (§ 3 písm. d) a § 6).
9. Spolupráce při zajištění auditu kybernetické bezpečnosti a implementaci nápravných opatření z auditních zjištění (§ 3 písm. e) a § 16 odst. 3).
10. Zajištění pravidelného vyhodnocování účinnosti ISMS a příprava zprávy o přezkoumání systému řízení bezpečnosti informací (§ 3 písm. f) a g)).
11. Koordinace řízení významných změn z pohledu kybernetické bezpečnosti a jejich dopadů na ISMS (§ 11).
12. Spolupráce na řízení kontinuity činností, zejména při analýze dopadů, tvorbě plánů kontinuity a jejich testování (§ 15).

13. Dohled nad plněním požadavků v oblasti bezpečnosti lidských zdrojů, zejména v oblasti bezpečnostního povědomí a školení (§ 10).
14. Koordinace spolupráce s dodavateli z pohledu kybernetické bezpečnosti a řízení souvisejících rizik (§ 9).
15. Dohled nad implementací technických a organizačních opatření napříč oblastmi vyhlášky (§ 17 až § 27).

Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti (dále jen „AKB") je pověřen návrhem implementace bezpečnostních opatření a zajištěním bezpečné architektury regulované služby. AKB odpovídá za technický návrh bezpečnostních opatření tak, aby byla zajištěna důvěrnost, integrita a dostupnost aktiv a aby implementovaná řešení odpovídala požadavkům právních předpisů a bezpečnostní politiky organizace.

Rozsah činnosti architekta kybernetické bezpečnosti dle VoKB 409/2025:

1. Návrh implementace bezpečnostních opatření v souladu se zákonem č. 264/2025 Sb. a VoKB 409/2025, včetně zajištění bezpečné architektury regulované služby (§ 5 odst. 2).
2. Návrh bezpečnostní architektury informačních a komunikačních systémů s ohledem na požadavky na důvěrnost, integritu a dostupnost aktiv (§ 7 a příloha č. 1).
3. Spolupráce na stanovení bezpečnostních požadavků při akvizici, vývoji a údržbě technických aktiv (§ 12 odst. 1 písm. c) a d)).
4. Návrh segmentace komunikační sítě a oddělení jednotlivých prostředí (produkční, testovací, zálohovací apod.) (§ 18 písm. a)).
5. Návrh bezpečných mechanismů pro řízení přístupu, autentizaci a správu identit (§ 13 a § 19).
6. Návrh bezpečnostních opatření pro ochranu komunikační infrastruktury, včetně řízení komunikace, vzdáleného přístupu a vzdálené správy (§ 18 písm. b) až d)).
7. Návrh použití kryptografických algoritmů, klíčů a certifikátů v souladu s požadavky vyhlášky (§ 25).
8. Spolupráce na návrhu opatření pro detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí (§ 21 až § 23).
9. Spolupráce na návrhu bezpečnostních opatření v oblasti aplikační bezpečnosti, včetně skenování zranitelností a penetračního testování (§ 24).
10. Návrh opatření pro zajištění dostupnosti regulované služby, včetně zálohování, redundance a obnovy (§ 26).
11. Posuzování dopadů významných změn na bezpečnost architektury a návrh odpovídajících bezpečnostních opatření (§ 11).
12. Spolupráce s manažerem kybernetické bezpečnosti při implementaci bezpečnostních opatření a řízení rizik (§ 8).
13. Poskytování odborných stanovisek k bezpečnostním aspektům technických řešení, projektů a změn v ICT prostředí organizace.
14. Spolupráce při řešení kybernetických bezpečnostních incidentů z pohledu návrhu nápravných a preventivních technických opatření (§ 14).
15. Zajištění souladu technických řešení s bezpečnostní politikou a bezpečnostní dokumentací organizace (§ 6).

Příloha č. 2 Specifikace dalších odborných služeb kybernetické bezpečnost

Aplikace pro monitorování kybernetické bezpečnosti
Právní základ: § 14, § 21, § 22 a § 23 VoKB č. 409/2025 Sb.

Monitoring kybernetické bezpečnosti zahrnuje detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí za účelem včasné identifikace kybernetických bezpečnostních incidentů a zajištění jejich účinného zvládání. Organizace je povinna zavést nástroje a procesy, které zajistí nepřetržitý dohled nad bezpečností regulované služby.

Poskytovatel zajistí pro Objednatele zpřístupnění a provoz softwarového řešení (dále jen „Aplikace"), určeného pro monitorování a podporu správy kybernetické bezpečnosti.

Rozsah činností v oblasti monitoringu kybernetické bezpečnosti dle VoKB 409/2025:

1. Zavedení nástroje pro detekci kybernetických bezpečnostních událostí, který zajišťuje kontrolu síťového provozu, komunikace na perimetru a aktivní blokování nežádoucí komunikace (§ 21 odst. 1).
2. Zavedení centrálně spravovaného nástroje pro detekci kybernetických bezpečnostních událostí na úrovni technických aktiv, včetně ochrany proti škodlivému kódu, sledování činností aplikací, procesů a uživatelů (§ 21 odst. 2).
3. Zajištění pravidelné a bezodkladné aktualizace nástrojů pro detekci kybernetických bezpečnostních událostí, včetně jejich nastavení a detekčních pravidel (§ 21 odst. 3).
4. Stanovení rozsahu technických aktiv, u kterých je prováděno zaznamenávání bezpečnostních a provozních událostí, a jeho pravidelná aktualizace (§ 22 odst. 1).
5. Zaznamenávání bezpečnostních a relevantních provozních událostí v komunikační síti, na síťovém perimetru a na určených technických aktivech (§ 22 odst. 2).
6. Zaznamenávání událostí zahrnujících zejména přihlašování a odhlašování, privilegované činnosti, změny oprávnění, pokusy o neoprávněný přístup, činnost technických aktiv a manipulaci se záznamy (§ 22 odst. 3).
7. Zajištění, aby zaznamenávané události obsahovaly identifikační údaje o činnosti, účtu, zařízení, čase a výsledku operace (§ 22 odst. 4).
8. Zajištění ochrany záznamů událostí z hlediska důvěrnosti a integrity a jejich ukládání v centralizovaném úložišti (§ 22 odst. 5 písm. a) a b)).
9. Uchovávání záznamů událostí po dobu alespoň 18 měsíců (§ 22 odst. 5 písm. c)).
10. Zajištění synchronizace času napříč technickými aktivy (§ 22 odst. 6).
11. Zavedení nástroje pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí, který umožňuje korelaci událostí, detekci incidentů a včasné varování odpovědných osob (§ 23 odst. 1).
12. Zajištění nepřetržitého monitoringu a vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů (§ 23 odst. 1 písm. c)).
13. Zajištění pravidelné aktualizace pravidel a nastavení nástroje pro vyhodnocování kybernetických bezpečnostních událostí a minimalizace nesprávného vyhodnocení (§ 23 odst. 2).

14. Využívání výstupů z monitoringu pro zlepšování systému řízení bezpečnosti informací (§ 23 odst. 3).
15. Zajištění návaznosti monitoringu na procesy zvládání kybernetických bezpečnostních událostí a incidentů, včetně jejich klasifikace, evidence a řešení (§ 14).

Aplikace je dostupná prostřednictvím webového rozhraní umožňujícího oprávněným osobám přístup ke statistikám, přehledům a analýzám bezpečnostních událostí. Součástí řešení může být instalace technických komponent na serverech nebo koncových zařízeních Objednatele v rozsahu nezbytném pro zajištění funkčnosti Aplikace.
Funkcionalita Aplikace zahrnuje zejména:

- automatizovaný sběr a vyhodnocování bezpečnostních událostí z vybraných zdrojů dat za účelem identifikace potenciálních bezpečnostních hrozeb,
- filtrování, třídění a evidenci bezpečnostních incidentů, včetně možnosti jejich kategorizace a přiřazování odpovědným osobám,
- podporu oznamování a evidence bezpečnostních událostí prostřednictvím webového rozhraní,
- generování auditních záznamů a reportů o stavu kybernetické bezpečnosti a zaznamenaných událostech.

Aplikace dále monitoruje mj.

- Neaktuální aktualizace OS/Windows
- Neaktuální aktualizace SW
- Neúspěšné přihlášení do Windows (např. podezřelé přístupy mimo pracovní dobu, více pokusů o přihlášení s nesprávným heslem)
- Varování před viry
- Vypnutý firewall
- Modifikace souborů nebo přístup do citlivých složek
- Spouštění neznámých procesů / skriptů
- Změny oprávnění jednotlivých uživatelů
- Vytváření nebo mazání uživatelských účtu
- Nebezpečné/nezabezpečené webové stránky
- Ověření šifrování disků (např. BitLocker)
- Připojení externích uložišť
- Instalace neautorizovaného nebo škodlivého softwaru
- Dodržování politiky hesel (složitost, pravidelná změna)
- Náhlý nárůst obsazeného místa na disku (indikace malwaru..)

Aplikace slouží jako nástroj podpory řízení kybernetické bezpečnosti manažera kybernetické bezpečnosti.

Rozsah monitorovaných systémů, zdrojů dat a nastavení vyhodnocovacích parametrů je určen dohodou smluvních stran.