Smlouva

o dodávce HW a migraci systému SIEM ArcSight, včetně rozšíření licence

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“),

mezi:

Českou národní bankou

Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel“ nebo také „ČNB“)

a

S&T CZ s.r.o.
se sídlem: V Parku 2316/12, 148 00 Praha 4
zastoupenou: Ing. Miroslavem Bečkou a Dušanem Stránským, jednateli společnosti
IČO: 44846029
DIČ: CZ44846029
bankovní spojení/číslo účtu: ČSOB, a.s.; č.ú. 117422733/0300

(dále jen „poskytovatel“)

Preambule

ČNB provozuje systém managementu bezpečnostních informací a událostí (dále jen „SIEM“) založený na platformě ArcSight. Podrobnější specifikace současného řešení objednatele je uvedena v příloze č. 2 této smlouvy. Jelikož výrobce oznámil ukončení vývoje produktů provozovaných na aktuální platformě, je nutné provést migraci do nové, a to včetně pořízení potřebného HW. Účelem této smlouvy je rovněž implementace nových programových prostředků a migrace stávající licence včetně jejího rozšíření, aby bylo možné zpracovávat větší množství záznamů v rámci SIEM. Níže uvedená smlouva tyto požadavky ČNB zabezpečuje.

Článek I
Předmět, rozsah a místo plnění

1. Poskytovatel se zavazuje dodat, nainstalovat a implementovat HW a SW komponenty blíže specifikované v příloze č. 1 této smlouvy a provést migraci stavající konfigurace, licence, kontentu a dat ze současného řešení SIEM objednatele založeného na platformě ArcSight v souladu s čl. II této smlouvy, včetně dodání příslušných licencí, které tuto implementaci plně pokrývají (dále též „dílo“).

2. Předmětem této smlouvy je dále závazek poskytovatele poskytovat objednateli podporu díla podle čl. VI této smlouvy, a to ode dne podpisu závěrečného akceptačního protokolu oběma smluvními stranami.
3. Plnění dle odstavce 1 tohoto článku musí splňovat funkční požadavky uvedené v příloze č. 2 této smlouvy.
4. Poskytovatel se zavazuje zajistit, že veškeré technické prostředky (HW), které jsou součástí díla, musí být nové a nepoužité (maximálně zahořelé z výroby, popř. zapnuté pro ověření funkčnosti) a musí být spolu s poskytnutými programovými prostředky (SW) výrobcem určeny pro evropský trh, pakliže výrobce takové určení provádí. Dodavatel je je po dobu účinnosti této smlouvy povinen na požádání objednateli doložit skutečnost, že HW a SW je určen pro evropský trh, pakliže výrobce takové určení provádí, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.
5. Poskytovatel se zavazuje v rámci realizace díla nainstalovat v prostředí objednatele nejnovější, stabilní verzi SW ArcSight, která bude výrobcem v době plnění uvedena na trh.
6. Místem plnění budou prostory výpočetního střediska v objektu objednatele na adrese: Na Příkopě 28, 115 03 Praha 1.
7. Předmětem této smlouvy je závazek objednatele poskytnout potřebnou součinnost a zaplatit za poskytnutá plnění ceny dle čl. V.
8. Poskytovatel bere na vědomí, že mu nebude umožněn vzdálený přístup k serverům objednatele.

Článek II
Průběh plnění

1. Plnění podle čl. I odst. 1 této smlouvy bude realizováno v následujících fázích, které budou předmětem akceptace podle článku IV této smlouvy, takto:
   a) **Fáze 1 – Realizační studie - vypracování detailního technického popisu cílového stavu a vypracování implementačního postupu**:

      Poskytovatel se zavazuje na základě analýzy systémového prostředí ČNB vypracovat realizační studii, ve které bude uveden podrobný implementační postup a detailní popis cílového stavu dodávaného díla. Realizační studie bude obsahovat minimálně:

      - detailní popis architektury systému dodávaného díla,
      - podrobný návrh postupu implementace díla (harmonogramu) s ohledem na dodržení požadavků na dobu omezení provozu stávajícího systému SIEM, uvedenou v odst. 2 tohoto článku,
      - podrobný návrh organizačního zabezpečení nezbytného pro provádění díla,
      - detailní návrh plánu zálohování konfigurace a kontentu dodaného díla,
      - popis nároků na poskytnutí nezbytné součinnosti ze strany objednatele,
      - popis akceptačních testů (funkční, zátěžové, obnovy po havárii apod.) nezbytných pro ověření splnění funkčních požadavků díla,

- podrobný harmonogram provádění všech dalších fází díla v prostředí ČNB při respektování lhůt dle čl. III odst. 1 této smlouvy,
- detailní specifikace 5 objednatelem definovaných scénářů (use cases), které budou vytvořeny v systému ArcSight Recon ve fázi 2. Tyto scénáře budou obsahovat sadu dashboardů, query, reportů a alertů,
- návrh a detailní specifikace 2 scénářů (use cases), které budou vytvořeny v systému ArcSight SOAR ve fázi 2.

Poskytovatel se zavazuje předat řádně zpracovanou realizační studii k dílčí akceptaci objednateli ve lhůtě stanovené v čl. III odst. 1 této smlouvy.

Řádně zpracovanou realizační studii předá poskytovatel objednateli v jednom vyhotovení v elektronické podobě v českém jazyce, ve formátech MS Office nebo PDF.

Lhůty v objednatelem akceptovaném harmonogramu v realizační studii budou pro poskytovatele závazné, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě písemně jinak (bez povinnosti uzavření dodatku), přičemž tato dohoda není možná ohledně lhůt stanovených v čl. III odst. 1 této smlouvy, které lze měnit objednatelem (pověřenou osobou) v souladu s odst. 3 tohoto článku.

b) **Fáze 2 – kompletní dodávka HW komponent a SW licencí, jejich instalace a konfigurace v systémovém prostředí ČNB.** Tato fáze 2 v sobě zahrnuje zejména následující kroky:

- kompletní dodávka 2 serverů pro systém SIEM včetně jejich instalace a konfigurace, instalace SW založeného na platformě ArcSight a migrace stávající konfigurace, licence, kontentu a dat. Součástí je zejména:
  - dodávka serverů s příslušenstvím dle specifikace uvedené v příloze č. 1 této smlouvy (dále jen „servery“) a splňující veškeré požadavky uvedené v příloze č. 2 této smlouvy,
  - instalace dodaných serverů do racku objednatele včetně připojení všech potřebných konektorů a přepínače KVM,
  - konfigurace BIOS serveru – doporučená nastavení s ohledem na výkon a power management,
  - konfigurace HW komponent serverů, zejména konfigurace lokálně instalovaných disků (SSD), konfigurace úložiště pro cold storage, nastavení požadovaného RAID a sítě,
  - konfigurace komponent pro vzdálený přístup k serverům,
  - instalace SW VMware vSphere a potřebných ovladačů HW komponent serverů, včetně licence,
  - vytvoření potřebných virtuálních serverů, včetně instalace dodaného operačního systému a potřebných ovladačů HW komponent serveru, včetně licence,
  - nastavení repository pro stahování updatů nainstalovaného operačního systému a provedení aktualizace,
  - hardening HW a SW na úroveň CIS L1,
  - instalace posledních verzí SW ArcSight vydaného výrobcem na dodaný HW dle specifikace stanovené v rámci přílohy č. 2 této smlouvy a konfigurace dle současného SW ArcSight, včetně migrace stávající licence ArcSight Logger do nové platformy ArcSight Recon,
  - upgrade ArcSight ESM na poslední verzi vydanou výrobcem,

- instalace nově dodaných licencí SW ArcSight,
- vytvoření uživatelských účtů v ArcSight Recon, při zachování schéma přístupu dle ArcSight ESM u práv k logům a kontentu,
- vytvoření 5 objednatelem definovaných scénářů (use cases) v systému ArcSight Recon, detailně specifikované v realizační studii,
- vytvoření 2 scénářů (use cases) v systému ArcSight SOAR detailně specifikovaných v realizační studii,
- migrace dat (logů) uložených v současném systému ArcSight logger do nového systému ArcSight Recon za posledních 12 měsíců,
- nastavení pravidelného zálohování konfiguračních souborů a kontentu všech komponent dodaného SW, konfiguračních souborů operačního systému a kopírování této zálohy na vzdálený server s OS Windows dle stávající instalace (pro komunikaci se vzdáleným serverem bude použit protokol CIFS [Common Internet File System]),
- změna konfigurace systému ArcSight Manager Center (ArcMC) související s jeho migrací do nové architektury na dodaný HW,
- provedení všech konfiguračních změn u sběru logů, souvisejících s migrací systému ArcSight logger do ArcSight Recon,
- vytvoření a předání dokumentace dodaného díla v el. podobě, ve formátech MS Office nebo PDF zahrnující minimálně:
    - popis funkčního schématu dodaného díla, včetně zapojení a konfigurace,
    - postup implementace díla,
    - postupy pravidelné údržby díla,
    - postupy diagnostiky a monitorování provozu systému díla,
    - postupy řešení havarijních stavů systému díla,
    - postupy zálohování, archivace a obnovy konfigurace systému díla a dat,
- zaškolení administrátorů (pracovníků objednatele) v rozsahu umožňujícím provádět:
    - běžný rutinní provoz a údržbu dodávaného díla,
    - řešení obvyklých problémů,
    - správu uživatelských oprávnění,
    - monitoring stavu dodaného díla,
    - zálohování a obnovu konfigurace a dat,
    - tvorbu pohledů, reportů, dashboardů apod.,
- provedení funkčních a zátěžových testů a testu obnovy po havárii uvedených v realizační studii.

c) Fáze 3 – ověřovací provoz:

- Po dobu 1 měsíce od podpisu dílčího akceptačního protokolu fáze 2 bude bez přerušení probíhat ověřovací provoz v režimu standardního provozu a za součinnosti poskytovatele, spočívající v odstraňování vad implementace a konfigurace za podmínek stanovených v čl. VI. Cílem je ověřit v delším časovém horizontu stabilitu a provozní spolehlivost díla.

2. Poskytovatel nesmí během implementace díla omezit provoz stávajícího systému SIEM a konektorů objednatele na více než 48 hod. kumulovaně za celou dobu implementace dle písm. b) předchozího odstavce. Každá z dílčích odstávek nesmí být delší než 8 hodin. Implementační práce budou probíhat ve standardní pracovní dobu objednatele, tj. pondělí

až pátek, od 7:45 do 16:15 hod. (dále také jen „pracovní doba objednatele“ nebo „pracovní hodiny“). Na základě výslovného písemného požadavku poskytovatele, a to formou e-mailové zprávy poskytovatele adresovaného pověřeným osobám objednatele uvedeným v článku III odst. 3 této smlouvy lze výjimečně dohodnout, že implemetační práce proběhnou i po skončení pracovní doby objednatele (tj. Po–Pá, po 16:15 hod.).

3. Lhůtu(y) uvedenou(é) v čl. III odst. 1 je oprávněna kterákoliv z pověřených osob objednatele, na písemnou a odůvodněnou žádost poskytovatele, přiměřeně okolnostem prodloužit, pokud poskytovatel objektivně nemohl pokračovat v plnění dle této smlouvy z důvodu, že mu objednatel neposkytl povinnou a nezbytnou součinnost, nebo z důvodu skutečností stojících na straně poskytovatele, které ani poskytovatel jednající s náležitou péčí nemohl předvídat a které sám nezpůsobil (včetně např. výpadku či zdržení v dodavatelsko-odběratelském řetězci, výpadku v pracovní síle poskytovatele z důvodu opatření uložených orgány veřejné moci, nikoli v důsledku protiprávního jednání poskytovatele, zdržení v plnění jiných smluvních partnerů objednatele, které se plnění dle této smlouvy dotýká a které nebylo způsobeno objednatelem). Písemná žádost poskytovatele musí obsahovat i návrh prodloužení lhůt(y), ten však není pro pověřené osoby objednatele závazný. Úprava lhůt(y) bude provedena formou dodatku k této smlouvě.

Článek III
Lhůty plnění, součinnost, pověřené osoby

1. Poskytovatel se zavazuje ukončit jednotlivé fáze díla a dílo předat objednateli v následujících lhůtách:
   a) plnění v rámci fáze 1 dle čl. II odst. 1 písm. a) této smlouvy, včetně její akceptace ze strany objednatele, je povinen ukončit **nejpozději do 20 pracovních dnů** ode dne účinnosti této smlouvy,
   b) plnění v rámci fáze 2 dle čl. II odst. 1 písm. b) této smlouvy, včetně její akceptace ze strany objednatele, je poskytovatel povinen ukončit **nejpozději do 29. 2. 2024,**
   c) plnění v rámci fáze 3 dle čl. II odst. 1 písm. c) této smlouvy, včetně její akceptace ze strany objednatele, je poskytovatel povinen ukončit a předat dílo objednateli v souladu s čl. IV odst. 4 této smlouvy nejpozději **do 40 pracovních dnů** ode dne akceptace fáze 2, nejdříve však dne 2. 1. 2024.
2. Objednatel se zavazuje vytvořit poskytovateli k instalaci a implementaci HW a SW dle této smlouvy potřebné podmínky, zejména:
   a) zajistit přístup odborných pracovníků poskytovatele ke klientskému zařízení, z něhož bude realizována implementace SW,
   b) připravit pro instalaci HW a SW potřebné technické prostředky (zasíťování + přidělení potřebných IP adres apod.).
3. Pověřenými osobami jsou:
   a) za objednatele:

b) za poskytovatele:

[redacted]

4. V případě změny pověřených osob smluvních stran nebo jejich kontaktních údajů jsou smluvní strany povinny nahlásit změnu následující pracovní den po provedení změny na e-mailové adresy pověřených osob druhé smluvní strany. Změna osob je účinná dnem jejího oznámení druhé smluvní straně, a to bez povinnosti uzavírat dodatek k této smlouvě.

Článek IV
Akceptace předmětu plnění smlouvy

1. Společně s řádně zpracovanou realizační studií předloží poskytovatel objednateli i návrh dílčího akceptačního protokolu za účelem akceptace realizační studie. Nejpozději ve lhůtě 5 pracovních dnů rozhodne objednatel o akceptaci studie podpisem dílčího akceptačního protokolu nebo studii odmítne akceptovat.

   Objednatel realizační studii akceptuje, pokud bude obsahovat všechny náležitosti stanovené v rámci čl. II odst. 1 písm. a) této smlouvy a návrh díla popsaný v realizační studii bude splňovat všechny podmínky stanovené v této smlouvě o dílo, včetně požadavků stanovených v rámci přílohy č. 1 a 2 této smlouvy.

   Do okamžiku akceptace fáze 1 je objednatel oprávněn smlouvu zrušit uhrazením odstupného v souladu s čl. XIII odst. 8 této smlouvy.

2. Po ukončení implementace díla a provedení testů dle fáze 2, uvedených v čl. II odst. 1 písm. b) této smlouvy, předloží poskytovatel výsledek jím provedených prací a testů objednateli k akceptaci. Akceptační řízení bude objednatelem provedeno do 5 pracovních dnů po dokončení implementace a provedení příslušných testů poskytovatelem. O výsledku akceptačního řízení fáze 2 bude objednatelem sepsán dílčí akceptační protokol, ke kterému vyjádří poskytovatel své písemné stanovisko nejpozději do 3 pracovních dnů od jeho obdržení. Poskytovatel je oprávněn s dílčím akceptačním protokolem vyjádřit souhlas také tím, že ve lhůtě dle předchozí věty žádné stanovisko neodešle.

3. V případě akceptace fáze 2 bude následující pracovní den zahájen ověřovací provoz – viz čl. II odst. 1 písm. c).

4. Po úspěšném ukončení ověřovacího provozu v rámci fáze 3 bude objednatelem sepsán závěrečný akceptační protokol, na základě kterého bude dílo předáno.

5. Pokud objednatel pro vady kteroukoliv fázi neakceptuje, uvede to v akceptačním protokolu spolu s odůvodněním. V případě akceptace kterékoliv fáze s drobnými vadami bude akceptační protokol obsahovat výčet vad, způsob a lhůtu pro jejich odstranění.

6. Objednatel převezme dílo pouze tehdy, pokud:

   - poskytovatel dodal, nainstaloval a implementoval veškeré HW a SW komponenty dle této smlouvy včetně jejich požadované konfigurace a provedl požadované testy jejich funkčnosti a zátěžové testy dle čl. II odst. 1 písm. b),
   - poskytovatel poskytl a implementoval licence VMware vSphere,
   - poskytovatel poskytl a implementoval licence dodaného operačního systému,

- poskytovatel poskytl a implementoval rozšíření licence ArcSight Recon, ESM a Intelligence,
- poskytovatel odstranil veškeré vady, které mu objednatel ohlásil v rámci všech tří akceptačních procesů, s výjimkou případu, kdy byla provedena akceptace s drobnými vadami,
- byly splněny veškeré požadavky objednatele uvedené v příloze č. 2 této smlouvy,
- provedl dílo v souladu s akceptovanou realizační studií, nebylo-li smluvními stranami dohodnuto jinak.

7. Poskytovatel plně odpovídá za to, že dodané dílo bude plně funkční a schopno použití v prostředí objednatele.

Článek V
Cena plnění a platební podmínky

1. Celková cena díla podle čl. I odst. 1 činí celkem **7 556 584 Kč bez DPH** včetně licencí, Bližší specifikace ceny díla a podpory je uvedena v příloze č. 3 této smlouvy.
2. Cena za podporu díla (dodaných HW komponent a SW licencí) dle čl. I odst. 2, s výjimkou ceny za podporu na místě, je stanovena paušálně a činí ročně **2 323 264 Kč bez DPH.** Z toho činí roční cena podpory HW částku ve výši **0 Kč bez DPH** a roční cena podpory SW částku ve výši **2 323 264 Kč bez DPH**.
3. Cena za podporu na místě dle čl. VI odst. 1 písm. c) této smlouvy v rozsahu 12 člověkodní ročně je stanovena paušálně a činí ročně **240 000 Kč bez DPH.**
4. Cena za podporu na místě dle čl. VI odst. 1 písm. c) této smlouvy nad limit stanovený v odst. 3 tohoto článku bude stanovena jako součin počtu skutečně odpracovaných hodin a hodinové sazby, která činí **2 500 Kč bez DPH.**
5. K cenám uvedeným v odstavcích 1 až 4 tohoto článku bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. Ceny zahrnují veškeré náklady poskytovatele spojené s plněním podle této smlouvy (včetně nákladů na náhradní díly HW dodávaných v rámci podpory, dopravy a ztráty času techniků na cestě).
6. Poskytovateli bude poskytnuta záloha ve výši 80 % z ceny díla v Kč bez DPH uvedené v odst. 1 tohoto článku, a to po podpisu dílčího akceptačního protokolu fáze 2 dle čl. IV odst. 2 této smlouvy objednatelem, nejdříve však dne 1. 1. 2024.
7. Daňový doklad na cenu díla podle odstavce 1 tohoto článku je poskytovatel oprávněn vystavit po podpisu závěrečného akceptačního protokolu objednatelem, přičemž v tomto daňovém dokladu bude odečtena záloha poskytnutá dle odstavce 6 tohoto článku.
8. Úhrada paušální ceny podpory dle odstavce 2 a 3 tohoto článku bude objednatelem hrazena předem následovně:
   - první daňový doklad je oprávněn poskytovatel vystavit po podpisu závěrečného akceptačního protokolu objednatelem a poskytovatelem dle čl. IV odst. 4, to za celý rok poskytování podpory a
   - další daňové doklady je poskytovatel oprávněn vystavit vždy nejdříve 14 dní před koncem předplacené doby podpory.
9. Cena za podporu na místě dle čl. VI odst. 1 písm. c) této smlouvy nad limit stanovený v odst. 3 tohoto článku bude objednatelem hrazena na základě daňového dokladu

vystaveného poskytovatelem nejdříve poslední den uplynulého kalendářního měsíce, ve kterém bylo příslušné plnění řádně poskytnuto. Kopie výkazu práce dle čl. VI odst. 9 podepsaného objednatelem bude tvořit nedílnou přílohu daňového dokladu.

10. Doklad k úhradě (fakturu) zašle poskytovatel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej poskytovatel v analogové formě na adresu:

    Česká národní banka
    sekce rozpočtu a účetnictví
    odbor účetnictví
    Na Příkopě 28
    115 03 Praha 1

11. Doklad k úhradě bude obsahovat údaje podle § 435 občanského zákoníku a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován poskytovatelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References), nebo číslo objednávky (ve formátu ISDOC v poli External_Order_ID ve skupině OrderReference), jsou-li objednávky v rámci smlouvy vystavovány. Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit poskytovateli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.

12. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřená osoba poskytovatele povinna na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle předchozí věty.

13. Splatnost daňového dokladu je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

14. Smluvní strany se dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.

15. Poskytovatel je oprávněn navrhnout změnu paušální ceny za podporu dle odst. 2 a 3 tohoto článku či hodinové sazby za podporu dle odst. 4 tohoto článku v návaznosti na vývoj indexu cen tržních služeb, stejné období předchozího roku = 100, konkrétně index „J62“ Služby v oblasti programování a poradenství, sloupec „Průměr od počátku roku“, a to průměr za předchozí kalendářní rok, který vyhlašuje Český statistický úřad. Ceny mohou být zvýšeny maximálně o částku odpovídající předmětné roční inflaci. Úprava ceny bude provedena formou dodatku ke smlouvě. První úpravu cen může poskytovatel navrhnout nejdříve 1 měsíc před uplynutím 1. roku od zahájení podpory dle čl. I odst. 2.

Článek VI
Podpora

1. Podpora díla dle čl. I odst. 2 této smlouvy zahrnuje:
   a) odstraňování jakýchkoliv vad dodaného HW,
   b) poskytování veškerých aktualizací dodaného i stávajícího SW ArcSight (nové verze, opravné verze, bezpečnostní záplaty),
   c) podporu v místě plnění, která bude spočívat zejména v následujících činnostech:
      1. řešení/odstraňování závad/problémů dodaného i stávajícího SW ArcSight,
      2. implementace aktualizací dodaného i stávajícího SW,
      3. konzultace v místě plnění zejména k problematice úpravy konfigurace, včetně doporučení na optimalizaci výkonu, úpravy kontentu, zvýšení dostupnosti a bezpečnosti celého díla apod.
2. Potřebu podpory ohlašuje objednatel poskytovateli telefonicky na telefonní číslo poskytovatele **296 300 500** s následným písemným potvrzením e-mailem na e-mailovou adresu poskytovatele **servicedesk@sntcz.cz** nebo pouze e-mailem na výše uvedenou e-mailovou adresu poskytovatele. Ohlášení učiněná po pracovní době objednatele se považují za ohlášení učiněná následující pracovní den, v čase odpovídajícím začátku uvedené pracovní doby objednatele.
3. Poskytovatel je povinen potvrdit přijetí ohlášení dle odst. 2 tohoto článku smlouvy **nejpozději do 6 pracovních hodin** od ohlášení, a to na e-mailovou adresu pověřené osoby objednatele dle čl. III odst. 3 této smlouvy, není-li v této smlouvě stanoveno dále jinak. Potvrzení přijetí ohlášení u podpory dle odst. 1 písm. a) nebo b) tohoto článku nemá vliv na lhůty stanovené v tomto článku.
4. Odstraňování vad HW dle odst. 1 písm. a) tohoto článku se zavazuje poskytovatel provádět v pracovní době objednatele v místě plnění s tím, že vady HW je povinen poskytovatel odstranit **nejpozději do 2 pracovních dnů** ode dne jejich ohlášení dle této smlouvy, nedohodnou-li se smluvní strany jinak.
5. V případě, že po odstranění vady HW nebude funkční SW nebo jeho část, případně dojde ke změně konfigurace serveru nebo některé HW komponenty, zavazuje se je poskytovatel uvést do funkčního stavu, a **to nejpozději do 1 pracovního dne** po odstranění vady HW nebo po ohlášení vady objednatelem dle této smlouvy, nedohodnou-li se smluvní strany jinak.
6. Poskytovatel poskytne objednateli aktualizace SW dle odst. 1 písm. b) tohoto článku **bez zbytečného odkladu, nejpozději však do 14 dnů** od uvedení výrobcem na trh, nedohodnou-li se smluvní strany jinak.
7. Poskytovatel je povinen nahlásit případnou změnu kontaktních údajů uvedených v odstavci 2 tohoto článku nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob objednatele. Změna je účinná dnem jejího oznámení druhé smluvní straně, a to bez povinnosti uzavírat dodatek k této smlouvě.
8. Podpora poskytovaná poskytovatelem musí vyhovovat technickým specifikacím a požadavkům výrobce dodaných HW a SW prostředků.
9. Konkrétní termín provedení podpory dle čl. VI odst. 1 písm. c) stanoví objednatel, nedohodnou-li se smluvní strany na konkrétním termínu. Poskytovatel vyhotoví o poskytnuté podpoře dle čl. VI odst. 1 písm. c) této smlouvy v daném měsíci "výkaz

práce", který bude obsahovat tyto údaje:

a. evidenční číslo požadavku,

b. stručná specifikace požadavku,

c. způsob vyřízení požadavku,

d. datum vyřízení požadavku,

e. celkový počet hodin/člověkodní provedené práce.

Správnost údajů uvedených ve výkazu práce bude potvrzena podpisem kterékoliv z pověřených osob za objednatele.

Článek VII
Přechod nebezpečí škody a vlastnické právo

Vlastnické právo k HW prostředkům dle této smlouvy přechází na objednatele dnem podpisu závěrečného akceptačního protokolu. SW prostředky poskytnuté podle této smlouvy je objednatel oprávněn užívat od okamžiku jejich instalace/implementace v místě plnění na dodávané HW prostředky. Nebezpečí škody na HW prostředcích přechází na objednatele dnem jejich instalace.

Článek VIII
Licenční ujednání

1. Poskytovatel poskytuje objednateli nevýhradní, nepřevoditelné, nedělitelné a časově ani teritoriálně neomezené oprávnění k výkonu práva užívat programové prostředky dodané dle této smlouvy a dle účelu této smlouvy. Právo užívání programových prostředků přechází na objednatele dnem jejich instalace/implementace na dodávané HW prostředky v místě plnění.
2. Dále poskytovatel poskytuje objednateli nevýhradní, časově a místně neomezené oprávnění užívat realizační studii, technické a provozní dokumentace dodané dle této smlouvy, a to i v podobě jakýchkoliv jejich návrhů, ke všem způsobům užití, zejména, avšak nikoliv výlučně, ke způsobům užití podle § 12 odst. 4 autorského zákona, kdy tato práva nabude objednatel okamžikem jejich poskytnutí poskytovatelem. Součástí této licence je i souhlas se zveřejněním (sdělováním veřejnosti) studie či dokumentací, a to i dálkově a hromadně účinným způsobem s tím, že poskytnutím studie či dokumentací objednateli se objednatel současně stává vlastníkem médií, na kterých jsou zachyceny. Objednatel může jakékoli oprávnění tvořící součást zde uvedeného oprávnění zcela nebo zčásti poskytnout třetí osobě, a to i bezúplatně. Objednatel je oprávněn sám nebo prostřednictvím třetí osoby studii nebo dokumentace nebo jejich části měnit, upravovat, zpracovávat, spojovat s jiným (autorským) dílem/prvky či zařazovat do (autorského) díla souborného.
3. Objednatel není povinen využít dle tohoto článku smlouvy poskytnuté licenční oprávnění ani zčásti.
4. Poskytovatel prohlašuje, že je právo dle odstavce 1 či 2 tohoto článku smlouvy oprávněn poskytnout a že na něm neváznou žádná práva třetích osob, která by poskytnutí bránila, jinak odpovídá za škodu tím způsobenou.
5. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace (tj. update/upgrade/patch/hotfix atd.).

6. Odměna za poskytnutí licencí podle této smlouvy je součástí cen podle čl. V této smlouvy.

Článek IX
Bezpečnostní požadavky objednatele

1. Poskytovatel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v příloze č. 4 této smlouvy.
2. Poskytovatel je v souvislosti s plněním této smlouvy dále povinen postupovat v souladu s obecnými pravidly v oblasti bezpečnosti IT, která tvoří přílohu č. 5 této smlouvy.

Článek X
Partnerství výrobce, osoby poskytovatele poskytující plnění

1. Poskytovatel se dále zavazuje, že plnění dle čl. I bude poskytováno pouze osobami splňujícími kvalifikaci požadovanou v bodu 8.3. zadávací dokumentace k veřejné zakázce s názvem „Dodávka HW a migrace systému SIEM ArcSight, včetně rozšíření licence“ (dále jen „veřejná zakázka“), na jejímž základě byla uzavřena tato smlouva, tj. že každá z těchto osob je certifikována k instalaci, implementaci a k provádění technické podpory HW a SW dle této smlouvy. Požadované certifikáty musejí být platné po celou dobu účinnosti této smlouvy. Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na výzvu objednatele tuto skutečnost doložit, a to do 5 pracovních dnů od doručení výzvy.
2. Změna v certifikovaných osobách dle předchozího odstavce poskytujících plnění může být provedena pouze se souhlasem objednatele, a to po splnění kvalifikačních požadavků objednatele ve stejném rozsahu, jaký byl stanoven v zadávacím řízení veřejné zakázky, nebude-li dohodnuto jinak. Odsouhlasení změny bude provedeno e-mailem alespoň jednou pověřenou osobou objednatele, bez povinnosti uzavřít dodatek k této smlouvě.
3. Objednatel si za splnění podmínek dle odstavce 1 tohoto článku vyhrazuje právo požádat o výměnu některé z certifikovaných osob z důvodu opakované nespokojenosti s kvalitou jí odváděné práce nebo nedostatečnou komunikací s objednatelem.
4. Za plnění poskytovaná poddodavatelem je poskytovatel odpovědný jako by toto plnění poskytoval sám.

Článek XI
Smluvní pokuty, úrok z prodlení

1. V případě, že poskytovatel nedodrží kteroukoli lhůtu pro předání plnění dle čl. III odst. 1, uhradí objednateli smluvní pokutu ve výši 1 000 Kč za každý den prodlení. To neplatí, pokud k prodlení poskytovatele došlo z důvodů na straně objednatele.
2. V případě prodlení poskytovatele ve lhůtě pro odstranění vady dodaného HW podle článku VI odst. 4, a to i dohodnuté mezi smluvními staranami, je objednatel oprávněn požadovat smluvní pokutu ve výši 3 000 Kč za každý pracovní den prodlení.
3. V případě prodlení poskytovatele ve lhůtě pro uvedení SW a konfigurace do funkčního stavu po odstranění vady dodaného HW podle článku VI odst. 5, a to i dohodnuté mezi smluvními staranami, je objednatel oprávněn požadovat smluvní pokutu ve výši 3 000 Kč za každý pracovní den prodlení.

4. V případě, že poskytovatel překročí maximální dobu omezení provozu SIEM během implementace dle čl. II odst. 2, uhradí objednateli smluvní pokutu ve výši 1 000 Kč za každou hodinu překročení.
5. V případě prodlení poskytovatele ve lhůtě pro potvrzení ohlášení podle čl. VI odst. 3 je objednatel oprávněn požadovat smluvní pokutu ve výši 100 Kč za každou pracovní hodinu prodlení.
6. V případě prodlení poskytovatele s poskytnutím aktualizace SW ve lhůtě dle čl. VI odst. 6, a to i dohodnuté mezi smluvními staranami, je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý kalendářní den prodlení.
7. V případě porušení kterékoliv povinnosti poskytovatele dle čl. IX je objednatel oprávněn požadovat smluvní pokutu ve výši 10 000 Kč za každý jednotlivý případ porušení.
8. V případě porušení kterékoliv povinnosti zhotovitele dle čl. X je objednatel oprávněn požadovat smluvní pokutu ve výši 40 000 Kč za každý jednotlivý případ porušení.
9. V případě prodlení poskytovatele v kterékoliv lhůtě dle čl. XII odst. 5 nebo 6 této smlouvy je objednatel oprávněn účtovat poskytovateli smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
10. V případě, že se ukáže tvrzení poskytovatele uvedené v čl. XII odst. 1, 2 nebo 4 této smlouvy jako nepravdivé nebo se ukáže pohlášení poskytovatele dle čl. VIII odst. 4 jako nepravdivé nebo poruší-li poskytovatel závazek stanovený v čl. XII odst. 3 této smlouvy, vzniká objednateli nárok na smluvní pokutu ve výši 100 000 Kč za každé jednotlivé nepravdivé tvrzení/prohlášení poskytovatele či za každé jednotlivé porušení závazku poskytovatele.
11. V případě porušení kterékoliv povinnosti poskytovatele podle čl. XII odst. 8 této smlouvy je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 500 Kč, a to za každý zjištěný případ takového porušení.
12. V případě prodlení objednatele s úhradou daňového dokladu má poskytovatel právo požadovat úrok z prodlení podle nařízení vlády č. 351/2013 Sb.
13. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů ode dne doručení platebního dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
14. Smluvní pokutou není dotčeno právo na náhradu škody v plné výši.

Článek XII
Další závazky poskytovatele

1. Poskytovatel potvrzuje, že ke dni účinnosti této smlouvy on ani jeho poddodavatelé nenaplňují definiční znaky subjektů uvedených v čl. 5k nařízení (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 833/2014“), nebo subjektů uvedených v čl. 1h rozhodnutí Rady 2014/512/SZBP ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále jen „rozhodnutí 2014/512/SZBP“), kterým je zakázáno zadat či plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu ve smyslu v tomto ustanovení uvedeného nařízení či rozhodnutí. Subjekty naplňující definiční znaky subjektů uvedených v čl. 5k nařízení č. 833/2014 nebo subjektů uvedených v čl. 1h rozhodnutí 2014/512/SZBP budou dále označovány jako „určené subjekty“.

2. Poskytovatel dále potvrzuje, že ke dni účinnosti této smlouvy není osobou uvedenou v příloze I nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „nařízení č. 269/2014“), nebo v příloze I nařízení Rady (EU) č. 208/2014 ze dne 6. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 208/2014“), nebo v příloze I nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska, ve znění jeho změn (dále také jako „nařízení č. 765/2006“), nebo v příloze rozhodnutí Rady 2014/145/SZBP ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „rozhodnutí 2014/145/SZBP“). Osoba uvedená v příloze I nařízení č. 269/2014 nebo v příloze I nařízení č. 208/2014 nebo v příloze I nařízení č. 765/2006 nebo v příloze rozhodnutí Rady 2014/145/SZBP bude dále označována jako „určená osoba“.
3. Poskytovatel se současně zavazuje, že určeným osobám dle předchozího odstavce (není-li jí sám) nebo v jejich prospěch nezpřístupní žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo.
4. Poskytovatel dále potvrzuje, že plnění jím poskytované dle této smlouvy neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie [tj. zejména zákazy dovozu výrobků ze železa a oceli ve smyslu nařízení Rady (EU) č. 2022/428 ze dne 15. března 2022, kterým se mění „základní“ nařízení (EU) č. 833/2014, nebo nařízení Rady (EU) č. 2022/355 ze dne 2. března 2022, kterým se mění „základní“ nařízení (ES) č. 765/2006 o omezujících opatřeních vzhledem k situaci v Bělorusku apod.]. Objednatel je oprávněn při porušení této povinnosti poskytovatele plnění nepřevzít v jakékoliv jeho části.
5. V případě, že by v průběhu účinnosti této smlouvy poskytovatel nebo jeho jakýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo se poskytovatel stal určenou osobou, je poskytovatel povinen o takové skutečnosti objednatele bez zbytečného odkladu, nejpozději do 2 pracovních dnů od nastání takové skutečnosti, písemně informovat.
6. Dojde-li za dobu účinnosti této smlouvy ke změnám v kterémkoliv z výše uvedených nařízení Rady (EU) či rozhodnutí Rady nebo k přijetí jakékoliv jiné nové legislativy tak, že bude nezbytné dát tuto smlouvu s nařízením Rady (EU), rozhodnutím Rady nebo jinou novou legislativou do souladu, zavazují se smluvní strany uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava či doplnění práv a povinností smluvních stran v rámci této smlouvy (sankční mechanismy či nové možnosti ukončení smlouvy z toho nevyjímaje), a to bez zbytečného odkladu, nejpozději do 15 pracovních dnů poté, co změny nařízení Rady (EU), rozhodnutí Rady či jiná nová legislativa nabudou platnosti, nedohodnou-li se smluvní strany jinak.
7. Vznikne-li objednateli v souvislosti s nepravdivým prohlášením nebo porušením povinností poskytovatele dle tohoto článku smlouvy jakákoliv škoda, je poskytovatel tuto škodu objednateli povinen v plné výši nahradit.
8. Poskytovatel se dále zavazuje, že v souvislosti s plněním této smlouvy:
    a) zajistí legální zaměstnávání osob a férové a důstojné pracovní podmínky pro všechny pracovníky podílející se na plnění této smlouvy. Férovými a důstojnými pracovními

podmínkami se přitom rozumí takové pracovní podmínky, které splňují alespoň minimální standardy stanovené pracovněprávními a mzdovými předpisy. Poskytovatel je povinen zajistit splnění požadavků dle tohoto ustanovení i u svých poddodavatelů;

b) zajistí řádné a včasné plnění finančních závazků vůči svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá dodavateli v souvislosti s touto smlouvou, a to nejpozději do 14 dnů od obdržení platby ze strany objednatele (pokud již splatnost poddodavatelem vystavené faktury nenastala dříve). Objednatel je oprávněn požadovat předložení dokladů o provedených platbách poddodavatelům.

Článek XIII
Doba trvání smlouvy, výpověď, odstoupení od smlouvy

1. Smlouva se v části poskytování podpory uzavírá na dobu neurčitou.
2. Smlouvu lze v části poskytování podpory ukončit písemnou výpovědí bez uvedení důvodu, která musí být doručena druhé smluvní straně nejpozději 6 měsíců přede dnem uplynutí předplacené doby podpory. Závazek poskytování podpory zaniká uplynutím posledního dne předplacené doby podpory.
3. V případě, že účinnost smlouvy skončí před koncem účtovacího období, vrátí poskytovatel objednateli alikvotní část předplacené ceny podpory.
4. Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to i v části, prostřednictvím písemného odstoupení. Takové odstoupení bude platné a nabude účinnosti dnem jeho doručení druhé smluvní straně.
5. Za podstatné porušení smlouvy strany považují zejména tyto případy:
   - ze strany poskytovatele:
     a) dodaný HW dle přílohy č. 1 této smlouvy nebude splňovat veškeré požadavky objednatele uvedené v příloze č. 2 této smlouvy,
     b) poskytovatel bude v prodlení s předáním díla nebo kterékoliv fáze díla dle čl. III odst. 1 delším než 30 dnů,
     c) poskytovatel bude v prodlení s odstraněním vady HW dle čl. VI odst. 4 nebo uvedením SW a konfigurace do funkčního stavu dle čl. VI odst. 5 delším než 30 dnů,
     d) nesplnění kterékoliv povinnosti poskytovatele dle čl. IX,
   - ze strany objednatele:
     a) prodlení s úhradou ceny plnění dle této smlouvy delší než 30 dnů.
6. Smluvní strany se dohodly, že je objednatel oprávněn odstoupit od smlouvy kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele.
7. Objednatel je oprávněn odstoupit od této smlouvy, a to i v její jakékoliv části, v případě, kdy na základě písemné informace od poskytovatele či z vlastní iniciativy shledá, že poskytovatel nebo jeho kterýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo poskytovatel se stane určenou osobou nebo poskytovatel neuzavře dodatek ke smlouvě ve smyslu čl. XII odst. 6 této smlouvy nebo poskytovatel poruší povinnost nezpřístupnit jakékoliv určené osobě (není-li jí sám) nebo v její prospěch žádné finanční

prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo, nebo povinnost dodat či poskytnout plnění, které neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie.

8. Objednatel je oprávněn vypovědět tuto smlouvu, a to i v její jakékoliv části, bez výpovědní doby v případě, kdy na základě písemné informace od poskytovatele či z vlastní iniciativy shledá, že poskytovatel nebo jeho kterýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo poskytovatel se stane určenou osobou nebo poskytovatel neuzavře dodatek ke smlouvě ve smyslu čl. XII odst. 6 této smlouvy nebo poskytovatel poruší povinnost nezpřístupnit jakékoliv určené osobě (není-li jí sám) nebo v její prospěch žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo, nebo povinnost dodat či poskytnout plnění, které neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie. Tato výpověď je účinná dnem jejího doručení poskytovateli.
9. Odstoupení od smlouvy se nedotýká nároku na zaplacení smluvní pokuty nebo nároku na náhradu škody vzniklé porušením smlouvy.
10. Smluvní strany si v souladu s ustanovením § 1992 občanského zákoníku sjednávají, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 30 000 Kč na účet poskytovatele, a to kdykoli do akceptace fáze 1. Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet poskytovatele. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti poskytovatele a případně vzniklé smluvní pokuty a náhrady škody.

Článek XIV
Uveřejnění smlouvy a skutečně uhrazené ceny

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.
3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XV
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
2. Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě uvedeno jinak. Dodatek v elektronické podobě se považuje za řádně podepsaný objednatelem, je-li podepsán kvalifikovanými elektronickými podpisy.

3. Závazkový vztah založený touto smlouvou se řídí českým právním řádem, zejména občanským zákoníkem a autorským zákonem.
4. Spory vyplývající z této smlouvy budou řešeny především dohodou smluvních stran. Nebude-li možné dosáhnout dohody, bude spor řešen před místně a věcně příslušným soudem České republiky, a to výlučně podle českého práva.
5. Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.
6. Smluvní strany vylučují uplatnění ustanovení § 1765 a § 1766 a § 2620 občanského zákoníku na svůj smluvní vztah založený touto smlouvou, čímž se ruší nárok dodavatele na jednání podle § 1765 odst. 1 občanského zákoníku. Poskytovatel tímto přebírá nebezpečí změny okolností dle § 1765 odst. 2 občanského zákoníku.
7. Práva a povinnosti vzniklé z této smlouvy mohou být postoupeny pouze po předchozím písemném souhlasu druhé smluvní strany.
8. Smlouva je vyhotovena v elektronické podobě, přičemž každá ze smluvních stran obdrží vyhotovení smlouvy opatřené elektronickými podpisy.
9. Nedílnou součástí této smlouvy jsou tyto přílohy:

Přílohy: č. 1 – Specifikace dodávaných HW komponent a SW licencí
č. 2 – Technické požadavky objednatele
č. 3 – Cenová tabulka
č. 4 – Bezpečnostní požadavky objednatele
č. 5 – Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

V Praze dne	V Praze dne
Za objednatele:	Za poskytovatele:
Ing. Milan Zirnsák ředitel sekce informatiky podepsáno elektronicky	Ing. Miroslav Bečka jednatel společnosti podepsáno elektronicky
Ing. Zdeněk Virius ředitel sekce správní podepsáno elektronicky	Dušan Stránský jednatel společnosti podepsáno elektronicky

Příloha č. 1

Specifikace dodávaných HW komponent a SW licencí

Produkt (P/N)	Popis produktu/služby
Server 1	
	"HPE Proliant DL385 Gen10 Plus V2 - P38411-B21 - 2x CPU AMD EPYC 7513 (32 jader @ 2,6 GHz) - 512 GB RAM (16x 32G) - řadič s 4GB cache - 5x 3,84 TB NVMe -- 11,5 TB v RAID5 3+1 + 1 spare - 2x 480GB SSD RI pro boot hypervizoru - LAN 4x 1Gbit - 2x zdroj - iLO Advanced - 5 let Tech Care Basic"
	Pig tail ke KVM USB+VGA
Server 2	
	"HPE Proliant DL385 Gen10 Plus V2 - P38411-B21 - 2x CPU AMD EPYC 7513 (32 jader @ 2,6 GHz) - 512 GB RAM (16x 32G) - řadič s 4GB cache - 5x 3,84 TB NVMe -- 11,5 TB v RAID5 3+1 + 1 spare - 2x 480GB SSD RI pro boot hypervizoru - LAN 4x 1Gbit - 2x zdroj - iLO Advanced - 5 let Tech Care Basic"
	Pig tail ke KVM USB+VGA
HW pro cold storage, včetně požadované úložné kapacity	
	"HPE MSA 2060 - R0Q77A - SAS 12Gbit konektivita - Dual kontrolér - 7x 20 TB NL SAS -- 80TB prostoru při RAID6 4+2 + 1x spare - podpora 5 let Tech Care Basic"
Produkt (P/N)	**Popis produktu/služby**
Licence podporovaného operačního systému na fyzických i virtuálních serverech	
G3J26AAE	RHEL Vrtl DC 2 Sckt 5yr 24x7 E-LTU
Licence VMWare vSphere Essentials plus Kit	
BD510AAE	VMw vSphere Ess 5yr E-LTU
Rozšíření licence ArcSight Logger o 5000 EPS	
SP-AH295	ArcSight Logger Standard Edition 5000 EPS SW E-LTU
Rozšíření licence ArcSight ESM o 500 EPS	
SP-AI107	ArcSight Enterprise Security Manager Standard Edition 500 EPS SW E-LTU

Licence ArcSight Intelligence, 500 Entit	
SP-AN162	ArcSight Intelligence Standard Edition for 500-5,000 Entities per anaged Entity SW E-LTU
Produkt (P/N)	**Popis produktu/služby**
Migrace systému SIEM do nové architektury	
SEC C3 + DCP	dle čl. II odst.1 smlouvy
Zaškolení administrátorů (pracovníků objednatele)	
SEC C3 + DCP	dle čl. II ods. 1 písm. b) smlouvy
Produkt (P/N)	**Popis produktu/služby**
Podpora dodaného HW	
	Podpora HW 5 let
Podpora dodaného SW	
SU-AA001	ArcSight Logger Standard Edition 5000 EPS SW E-LTU Business Support (SP-AH295), 48 měs.
SU-AA001	ArcSight Enterprise Security Manager Standard Edition 500 EPS SW E-LTU Business Support (SP-AI107), 48 měs.
SU-AA001	ArcSight Intelligence Standard Edition for 500-5,000 Entities per anaged Entity SW E-LTU Business Support (SP-AN162), 48 měs.
Podpora stávajícího SW (ESM-1000 EPS, Logger 925 EPS)	
Licence Q-Q-583216	Podpora stávajících licencí 48 měs.
Produkt (P/N)	**Popis produktu/služby**
Paušální cena podpory na místě	
SEC MD C3	MD SEC 12 člověkodnů ročně, celkem 4 roky
Produkt (P/N)	**Popis produktu/služby**
Podpora na místě nad 12 člověkodnů	
SEC MD C3	Cena za 1 hodinu 48 hodin ročně, celkem 4 roky

ArcSight Intelligence Behavioral Analytics

opentext™ | Cybersecurity

Flyer

ArcSight Intelligence Behavioral Analytics

ArcSight Intelligence behavioral analytics gives you a new lens through which to detect, investigate, and respond to threats that may be hiding in your enterprise—before your data is stolen.

Using machine learning, ArcSight Intelligence by OpenText™ distills billions of events into a prioritized list of high-quality security leads to focus and accelerate the efforts of your security operations center (SOC). ArcSight Intelligence's machine learning models, combined with a highly intuitive user interface (UI), accelerate threat detection and investigation from weeks to minutes.

Why ArcSight Intelligence

Many organizations have important assets to protect, whether it is customer information, intellectual property, critical infrastructure controls, or all of the above. Unfortunately, existing approaches to protecting these assets continuously fall short, leaving security teams to contend with rigid, rules-based analytics, fragmented security ecosystems, and a never-ending barrage of alerts—most of which are false alarms. Meanwhile, these teams are expected to flawlessly protect against critical threats like data exfiltration and unauthorized network access.

ArcSight Intelligence is uniquely positioned to find the threats that matter for enterprises with valuable data to protect, limited security or financial resources, and significant surface area to monitor. Unlike other solutions, ArcSight Intelligence bypasses rules and thresholds and instead assesses the potential risk of a user or entity in your enterprise based on mathematical probability and unsupervised machine learning models. This approach, combined with ArcSight Intelligence's native big-data architecture, allows your security team to detect threats with speed and at scale.

Detect. Investigate. Respond.

Figure 1. ArcSight Intelligence views your existing security data through a new lens in order to identify hidden threats by looking for anomalous behavior. This produces high-quality threat leads, allowing your security teams to respond and remediate quickly and effectively.

Using unsupervised machine learning—a type of artificial intelligence (AI) that doesn't need labels—ArcSight Intelligence's algorithms extract available entities (users, machines, IP addresses, servers, printers, etc.) from within log files and observe events that involve these entities to determine expected behavior—a measurement we call "unique normal." As new information comes through the analytics process, events are evaluated

Threat Detection Use Cases

Insider Threat
- At-Risk employee
- High-Risk Employees
- Account Misuse
- Privilege Account Misuse
- Terminated Employee Activity

Data Breach
- Data Staging
- Data Exfiltration
- Email Exfiltration
- Print Exfiltration
- USB Exfiltration
- Unusual data access
- Unusual uploads

Advanced Threat
- Compromised Account
- Internal Recon
- Unusual Traffic
- Abnormal Processes
- Unusual Applications
- Infected Host
- Malicious Tunneling
- Bot Detection

IP Theft
- Mooching
- Snooping
- Interactions with dormant resources/files
- High Risk IP/Data Access
- Lateral Movement

Figure 2. ArcSight Intelligence uses advanced mathematical algorithms to constantly mine billions of data points and reveal indicators of insider threats, data breaches, advanced persistent threats (APT), IP theft, and more.

against previously observed behavior to assess potential risk.

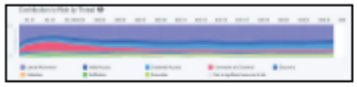
With this process of baselining and scoring, ArcSight Intelligence boosts the efficiency and speed at which security teams detect, triage, investigate, and respond to threats. ArcSight Intelligence's output risk assessments can be used to initiate actions via automation, orchestration, and alerting solutions to execute faster-than-human actions as risks are found. ArcSight Intelligence also provides downloadable reports summarizing immediate organizational risks.

Viewing Risky Entities

As a security practitioner, your primary mechanism for interacting with ArcSight Intelligence is the intuitive, web-based dashboard. ArcSight Intelligence's dashboard allows users to quickly and easily determine which entities represent the greatest potential risk. As entities are identified, the dashboard allows you to drill down into results so that the potential risk can be understood in the context of the generated alerts and, if desired, the raw events that produced them. The screenshots below show a drilldown from the list of riskiest users down to the raw events.

1. View all entities within the enterprise with analytics to display, grouped by entity type. The screenshot shows a list of users, with a presentation that displays them in order of risk score from highest to lowest.

2. When any entity is viewed, its risk score over time is displayed in a timeline view. This perspective shows not only the change in risk score, but also broadly characterizes the types of behavior that drove it.



3. When viewing an entity, a display of the alerts associated with the entity can be seen below the timeline view. They can be filtered by associated entities and types of risk and, because they display in chronological order linked to the timeline view, it is simple to see a narrative of the unfolding behavior in the context of other events.

4. Clicking on any of the alerts allows for examination that shows the event in context of the user's baseline and other relevant entities in the enterprise. The risk associated with the alert is displayed, and the model that triggered the alert is described in detail. Note that the user's baseline is compared to both itself, as well as to other similar entities. These similar entities are identified through statistically determined peer groups.

5. The raw events that triggered an alert are only one click away. In addition to seeing the actual contents of the log file responsible for the analytics, users have the ability to enter additional queries using this interface.

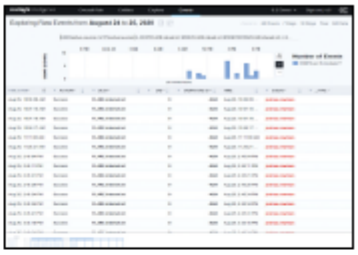


Table 1. Screenshots of the ArcSight Intelligence dashboard showing navigation through the analytical results

ArcSight Recon

CyberRes

Data Sheet

ArcSight Recon

Micro Focus ArcSight Recon is a comprehensive SIEM log management tool and security analytics solution that eases compliance burdens and accelerates forensic investigation.

Product Highlights

Cyber-security has never been more important. More business is conducted online, more sensitive information is stored digitally, and more work is completed by remote workforces than ever before. Compliance mandates are getting stricter, all while bad actors develop increasingly sophisticated methods of infiltration.

As organizations strive to collect and store security data from a seemingly infinite number of sources, data monitoring and management has become increasingly difficult. Many solutions in the market simply weren't built with security in mind, and inadvertently cause inefficiencies when implemented within the context of SIEM, security compliance, event logging, and forensic investigation. Logging and forensic investigation are essential tasks in a modern SOC, and organizations need a solution that transcends the standards of today in order to be equipped for tomorrow.

ArcSight Recon is a comprehensive log management and security analytics solution that eases compliance burdens and accelerates forensic investigation for security professionals. It combines the compliance, storage and reporting needs of log management with the capabilities of big-data search and analysis. Recon is built for security event logs and is therefore more intuitive and accessible for security analysts, it won't require a DBA to operate. It helps hunt and defeat threats by unifying data logs from across organizations, processing billions of events, and quickly making them available

for search, visualization and reporting. Recon helps SOC engineers gain a deeper understanding of alerts across their organization and plays an important role in ArcSight's mission to deliver powerful layered analytics.

Key Benefits

Centralize Log Management

ArcSight Recon stores terabytes of machine data from any source including logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, and cloud services. It enables you to store, search, monitor, and analyze data to gain centralized security intelligence from across your entire organization. For quick exploration of the data, Recon's event detail panel allows investigation of individual and grouped events. The raw message view allows analysts to inspect original, unformatted event logs. It was built with simplicity, usability and security in mind, and won't require a DBA to operate.

Key Features

- Event detail panel
- Raw message view
- Outlier detection
- User-friendly search bar
- 100+ out of the box reports and dashboards
- Unified ArcSight platform
- Single ID login

Key Benefits

- Centralize log management
- Hunt and defeat threats faster
- Security focused compliance
- Customize reports and dashboards
- Store data at scale
- Integrate with your security environment

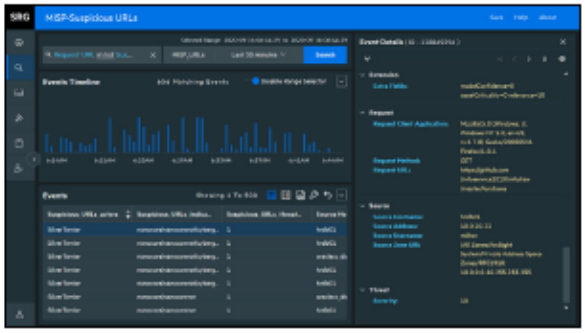


Figure 1. Event detail panel

Figure 2. GDPR Reports

Hunt and Defeat Threats Faster
Sift through mountains of log data with minimal effort using Recon's dynamic query suggestions and get results faster with its powerful security analytics technology. ArcSight Recon's columnar database responds to queries faster than traditional databases, enabling it to quickly and efficiently investigate millions of events. Storing clean, structured data in one centralized location accelerates investigation and improves the quality of results. Outlier detection provides visualizations to quickly identify deviations from baseline host behavior metrics. Recon's user-friendly search interface displays a grid or message view as well as a time-based histogram. It facilitates threat hunting in massive datasets, enabling security analytics at scale. It minimizes requirements for expertise and training, prioritizes abnormalities, and improves efficiency.

Security Focused Compliance
Prepare compliance reports faster with Recon's reporting content packages. Select the report wizard or choose a template to create crosstab reports, tables, or chart-based reports for your organization. After making your own customized reports, you can simultaneously email, upload and publish the reports as needed. You can also schedule your reports to be automatically generated and delivered to your peers and stakeholders, or to multiple recipients at once.

Recon reduces the pain and complexity of reporting with simpler, automated, customizable reports and dashboards. Pre-built content for FIPS 140-2, GDPR, PCI and IT-GOV compliance packages are now available, and more reporting templates expected in subsequent releases.

Recon comes with 100+ out of the box reports/dashboards including MITRE ATT&CK, Cloud, OWASP, data modeler and as an additional feature it supports external data sources like Text/Excel/Directory/Elastic

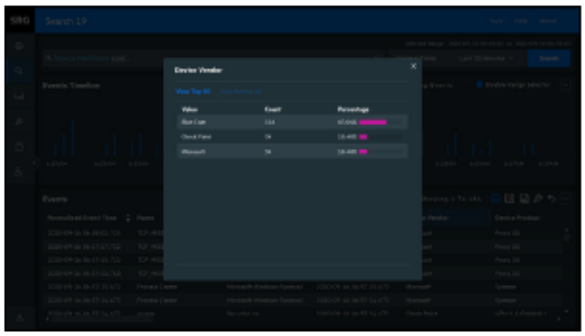


Figure 3. Histogram of vendor device values

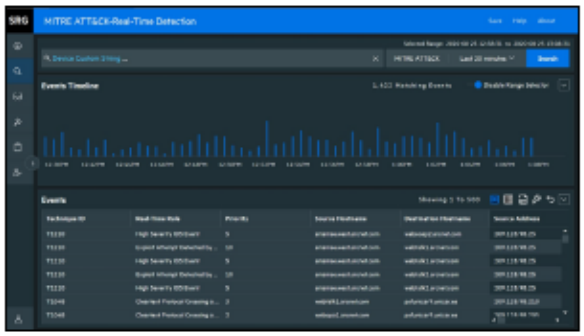


Figure 4. Pre-built MITRE ATT&CK content

Contact us at **CyberRes.com**
Like what you read? Share it.

search/JDBC, Rest JSON, XML. With the MITRE ATT&CK content, you can quickly see how much coverage you have against the tactics and techniques within the framework, and the reports show your tailored results in the context of MITRE techniques. Recon helps your security team to identify the risks, prioritize them and take action timely.

Store Data at Scale
Store data more efficiently with Recon's event aggregation and log compression. ArcSight Recon cost-effectively stores your security event log data, thanks to its impressive compression ratios. ArcSight SmartConnectors allows aggregation and filtering of events for additional log storage savings. Whether you choose to deploy with one node or multiple, ArcSight Recon is built to scale with your needs.

Integrate with Your Security Environment
Disparate, unstructured storage delays investigation and limits the ability to connect patterns or multi-stage attacks. Gain a complete view of security events by integrating with and consolidating your existing security operations solutions. ArcSight Recon leverages the Security Open Data Platform (SODP) architecture that allows you to collect, normalize, aggregate, and enrich data from over 480 source types. With the ArcSight 2021.1 release, you can now natively deploy Recon to your Azure and AWS environment to provide flexible architecture to your security posture.

Recon empowers teams to securely store data on its structured data lake for data exploration. Collect once, store once, and use your data often. With this unification you can now navigate between ArcSight ESM, ArcSight Intelligence and ArcSight Recon with a simple click of a button. ArcSight's single ID login (customizable) saves time when toggling between any of the ArcSight portfolio products. For organizations that utilize multiple solutions, Recon can also integrate with leading security tools to provide quick investigation, streamlined workflows and fast response times.

Why ArcSight?
The ArcSight next-gen SIEM platform is scalable and powerful. It is a comprehensive solution developed for security professionals by security experts. It takes a holistic approach to security intelligence, uniquely unifying Big Data collection, network, user and endpoint monitoring and forensics with advanced security analytics technologies, including hunt, investigation, and UEBA solutions. It provides real-time threat detection and response, compliance automation and assurance, and IT operational intelligence to provide a powerful layered analytics approach that enables the self-defending enterprise. While many vendors claim to provide a robust SIEM solution, the ArcSight team has the security expertise, experience, and leadership that few vendors can match. Our next-gen solution, proven methodologies, and 20 years of experience with some of the largest, most complex SOCs in the world make Micro Focus uniquely qualified to help you achieve greater security posture and operational excellence.

Learn more at
www.microfocus.com/en-us/cyberres/secops/arcsight-recon

CyberRes
A Micro Focus Line of Business

Příloha č. 2

Technické požadavky objednatele

1. Preambule

ČNB provozuje systém SIEM ArcSight v konfiguraci:

a) SW: ArcSight ESM v. 7.4.0, 1000 EPS

   HW:
   - HP ProLiant DL380 Gen10 Server
   - 1 x CPU Intel Xeon-Gold 5218
   - RAM 384 GB (12 x 32 GB)
   - 8x 3,2 SAS MU SFF SC SS540 SSD (19.2 TB RAID 6)
   - Rack mount 2U
   - 2x 500W platinum power supply
   - Licence iLO advanced remote management
   - Licence Red Hat Enterprice Linux 6.9 64-bit

b) SW: ArcSight Logger 7.2.2, 925 EPS
   Security ArcSight Connectors 7.14.0 a novější

c) SW: ArcSight Management Center 3.1.0
d) SW: ArcSight SmartConnectors 8.3.3

1.1 Obecné požadavky

ČNB požaduje provést migraci stávajícího systému SIEM do nové platformy, jejíž součástí je:
- Dodávka HW, včetně instalace hypervizoru VMware a virtuálních serverů s podporovaným operačním systémem, licence a konfigurace,
- instalace nových verzí SW ArcSight, včetně jeho konfigurace a migrace stávajících licencí,
- vytvoření definovaného kontentu v ArcSight Recon a ArcSight SOAR, dle specifikace v realizační studii,
- migrace dat z ArcSight Logger do nového systému ArcSight Recon,
- rozšíření stávající licence,
- provedení všech konfiguračních změn, souvisejících s migrací systému ArcSight logger do ArcSight Recon.

Hlavní komponenty ArcSight CDF (nová platforma):
- ArcSight Transformation HUB – zabezpečení příjmu událostí od konektorů a uložení do interní databáze,
- ArcSight Fusion – jednotná webová konzole obsahující všechny komponenty,
- ArcSight ESM – zabezpečuje korelaci jednotlivých událostí, předpokládá se nahrazení systémem ArcSight Detect,
- ArcSight Recon – systém pro rychlé vyhledávání auditní stopy, nahrazuje původní ArcSight Logger,

- ArcSight Intelligence (UEBA - User Entity and Behavioral Analytics) – komponenta umělé inteligence, která pomocí analýzy chování detekuje drobné anomálie, které nelze standardně při korelaci postihnout,
- ArcSight SOAR – systém pro automatizaci a orchestraci bezpečnosti,
- ArcSight Management Center – systém centrální správy inteligentních konektorů,
- ArcSight Galaxy.

1.2 Požadavky na dodávané servery

Server platformy x86/x64 velikosti 2U, který musí být certifikován výrobcem/dodavatelem pro provoz hypervizoru VMware a dodaného operačního systému a musí být podporován provoz SW platformy ArcSight.

Server bude dodán zkompletovaný (osazení RAM, CPU, disků, rozšiřujících karet atd.), nový a nepoužitý (maximálně z továrny zahořelý z výroby), popř. zapnutý pro ověření funkčnosti v rámci případné kompletace serveru prodávajícím před dodáním.

Server musí být vybaven software, který umožní konfiguraci jeho komponent (zejména interních pevných disků). Software může být dodán např. na CD/DVD, USB Flash-disku či může být nahrán přímo v serveru (ne však na interních discích serveru). Popřípadě je zpřístupněn odkaz na Internetu, kde je možné tento software stáhnout.

Server musí mít k dispozici komponentu (integrovanou či jako externí kartu/komponentu) pro vzdálený přístup k serveru v případě výpadku serveru (viz 1.2.6).

V případě, že jsou u serveru instalovány rozšiřující karty do PCI slotů, budou od výrobce či poskytovatele umístěny do správných pozic z hlediska maximálního využití komunikační rychlosti slotů a rozšiřujících karet, rozložení komunikační zátěže na různé interní kanály serverů, k nimž jsou dané sloty připojeny atd. Obdobně je totéž požadováno v případě interních disků osazených do serverů a paměti RAM.

Vzhledem k zamýšlenému použití serveru a na základě dosavadních provozních zkušeností ČNB byly stanoveny tyto **minimální** parametry serveru:

Server 1

provedení serveru	montovatelný do racku – velikost **2U**
procesor	Počet patic: 2 Počet CPU: 2 Platforma: x86-64 Počet fyzických jader: 32 jader / CPU, core min 2,0 GHz
RAM	Minimálně **512 GB** DDR4, min. 3 200 MT/s RDIMM
LAN	2x připojení GigaBit Ethernet (dvojice portů bude konfigurována jako fail-over pár), konektor je typu RJ-45
SSD	Minimálně **10 TB** chráněné užitné kapacity (RAID5), pro zajištění dostatečného IO výkonu
Boot	Minimálně 2x 480GB M.2 SSD RI v RAID1, formou PCIe karty nebo interního bootovacího zařízení

Server 2

provedení serveru	montovatelný do racku – velikost **2U**

procesor	Počet patic: 2 Počet CPU: 2 Platforma: x86-64 Počet fyzických jader: 32 jader / CPU, core min 2,0 GHz
RAM	Minimálně **512 GB** DDR4, min. 3200 MT/s RDIMM
LAN	2x připojení GigaBit Ethernet (dvojice portů bude konfigurována jako fail-over pár), konektor je typu RJ-45
SSD	Minimálně **10 TB** chráněné užitné kapacity (RAID5), pro zajištění dostatečného IO výkonu
Boot	Minimálně 2x 480GB M.2 SSD RI v RAID1, formou PCIe karty nebo interního bootovacího zařízení

K dodávaným serverům požadujeme dodat min, 80 TB úložné kapacity pro cold storage, která bude připojitelná k oběma serverům (RAID6, minimálně SATA).
Jejich technické provedení bude záviset na zvolené architektuře dodavatele.

1.2.1 Procesory

Procesory musí podporovat provoz 64-bitové verze operačního systému.

Procesory musí podporovat virtualizační technologie – viz např. AMD-V, Intel-VT.

Pro podporu virtualizace je nutno mít možnost v BIOSu serverů aktivovat tzv. „DEP – Data Execution Prevention“.

1.2.2 RAM

Paměť serveru je potřeba osadit tak, aby byla maximálně využita rychlost přítupu k pamětěm a zároveň bylo osazení cenově co nejefektivnější.

1.2.3 CD/DVD – ROM/RW

K serveru musí být připojitelná přes USB port externí DVD-ROM či RW mechanika, ze které musí jít server také nabootovat z bootovacího média operačního systému.

1.2.4. SATA

Požaduje se použití datových modulů typu SATA pro serverové použití certifikované výrobcem dodávaného HW (serverů).

Požadavek na úložnou kapacitu pro cold storage je míněn objednatelem jako čistá kapacita (kapacita volná pro uložení dat) sestavená z instalovaných SATA disků a chráněná vyžadovanou formou RAID

Pro dosažení požadované kapacity nelze použít žádnou formu HW či SW komprese dat.

1.2.5 SSD

Požaduje se použití datových modulů typu SSD, založené na technologii SAS (Serial Attached SCSI) – 2.5’’ provedení. Disky musí mít dvoukanálové připojení min. **12Gbps.** Připouští se možnost využití NVMe.

Instalovaný řadič/e disků:

- musí být osazeny minimálně 4 GB paměti cache a musí mít alespoň 2 nezávislé kanály pro komunikaci se skupinami SSD;
- musí mít chráněnu svou cache před nenadálým výpadkem napájení serveru, tj. řadič umožní udržení informací nezapsaných na SSD při výpadku napájení po dobu minimálně 48 hodin nebo potřebné informace dokáže včas zapsat na vlastní instalované SSD. Po připojení serveru na napájení tedy server pak korektně obnoví svou činnost s nakonfigurovanými disky;
- musí podporovat „write-through" mód a S.M.A.R.T (https://cs.wikipedia.org/wiki/S.M.A.R.T.)

Požadavek na chráněnou kapacitu u jednotlivých serverů je míněn objednatelem jako čistá kapacita (kapacita volná pro uložení dat) sestavená z instalovaných SSD a chráněná vyžadovanou formou RAID

Každá požadovaná skupina disků musí být opatřena min. 1 spare diskem odpovídající technologie a kapacity, který je připraven a konfigurován na okamžitou náhradu vadného disku. Kapacita spare disku nesmí být započtena do požadované kapacity.

Pro dosažení požadované kapacity nelze použít žádnou formu HW či SW komprese dat.

Dodané HDD podporují technologie Hot swapping, Hot-plug.

„Interní disk" je chápán jako disk zapojený do příslušné pozice uvnitř šasí serveru.

1.2.6 Management – Komponenta pro vzdálený přístup

Tato komponenta (integrovaná či řešená jako externí karta v PCI slotu) musí podporovat zejména následující funkce:

- podpora funkce virtuální CD/DVD mechaniky a z této virtuální mechaniky musí být také server bootovatelný a musí z něj být možno nainstalovat operační systém či virtualizační platformy certifikovanou pro daný server,
- přístup k serveru/komponentě prostřednictví dedikovaného LAN portu (povolený protokol pouze TCP/IP, Ethernet, 100Base-T) bez ohledu na stav operačního systému na něm provozovaném,
- podpora virtuální konzole – zobrazení obrazovky serveru prostřednictvím WWW prohlížeče (MS Edge, Chrome, apod.)
- HW vypnutí/zapnutí serveru či jeho restart,
- přístup musí být protokolem HTTPS/SSL a účty administrátorů musí být zabezpečeny heslem,
- filtrování příchozích adres (Firewall/IP tables) není požadováno,
- použití komponent Java a ActiveX na straně www prohlížeče vzhledem ke špatným zkušenostem z minulosti (u několika výrobců) není přípustné,
- odesílání auditních záznamů na vzdálený syslog server.

Komponenta nemusí mít od serveru oddělené samostatné elektrické napájení.

Komponenta musí být dostupná samostatným LAN portem (konektor RJ-45) – sdílení se standardním LAN portem není povoleno.

Při přihlášení do komponenty musí být umožněno pro zadání hesla použít z klávesnice PC všechny znaky, jež jsou povoleny pro heslo při přihlášení v operačním systému MS Windows 7 (tedy třeba i „*“).

1.2.7 Redundance, Pre-Failure záruka

Server bude mít redundantní komponenty chlazení a napájení, aby při výpadku jedné z nich dál server bez problémů fungoval

Na základě informací poskytnutých managementem (viz 1.2.6) či jinou formou automaticky dodanou se serverem je požadována minimálně pro SSD a RAM tzv. předporuchová záruka. Tj. management či jiný systém hlídá parametry uvedených zařízení a jejich trend a aktivně sám avizuje ještě před poruchou možnost výpadku dané komponenty. Pro ostatní komponenty (např. CPU a zdroje) musí být zajištěn reporting poruch nebo výpadků na těchto komponentách (není požadována pre-failure záruka).

Takovéto hlášení/report je pak poskytovatelem uznán jako důvod k výměně serveru či jeho komponenty.

1.2.8 Konektory, USB

Server musí standardně disponovat alespoň 4 USB porty, z toho alespoň jeden musí být dostupný na předním panelu serveru a nejméně 2 na zadní straně serveru.

Server musí mít k dispozici na zadní straně:

- oddělené konektory PS/2 pro připojení klávesnice a myši nebo USB port pro připojení do KVM switche – viz 1.2.11,
- VGA konektor pro připojení monitoru, resp. KVM switche viz 1.2.11.

1.2.9 Výška serveru, instalace do racků a další požadavky

Poptávaný server bude instalován do standardního 19'' racku a musí mít sání studeného vzduchu zepředu a vyfukování teplého vzduchu dozadu.

Součástí dodávky serveru bude i kit/sada pro namontování serveru do racku. Její součástí budou zejména:

- kolejničky instalované do standardního racku a komponenta(y) na boky serveru pro namontování serveru do racku. Kolejničky musí být ve verzi instalovatelné bez dalšího spojovacího materiálu (šroubky, „oříšky“, apod.). Pozn.: Kolejničky mají na obou koncích háčky (s pojistkou), které zapadají přímo do dírek na bočních sloupcích racků. Kolejnička má proměnnou délku, takže je možné ji využít u racků s různou hloubkou a pro její osazení není potřeba žádný spojovací materiál.
- ramínko instalované na zadní stranu serveru pro umístění kabeláže (LAN, připojení ke KVM, elektrické kabely), které umožní vysunout server po kolejničkách ven z racku, aniž je nutno odpojit server od těchto kabelů.

Účelem tohoto kitu pro namontování serveru do racku je schopnost zaměstnanců ČNB při opravách či údržbě serveru jeho vytažení z racku po kolejničkách tak, že je možno

otevřít kryt serveru a realizovat potřebné práce. A to vše aniž je nutno vzadu odpojit server od kabeláže k tomuto serveru připojené.

1.2.10 Napájení

Napájecí zdroje musí být připojitelné na rozvod elektrického napětí 230V.

Pro každý napájecí zdroj dodaného serveru bude v dodávce přívodní napájecí kabel s koncovkami IEC 60320 C13/C14 v délce nejméně 1 m.

1.2.11 KVM

Server bude připojený na přepínač klávesnice/myš/monitor (CAT5 0x1x8 KVM Server Console Switch), který je založen na LAN připojení (metalické, konektor RJ-45). Komponenty pro připojení serveru ke KVM jsou součástí dodávky.

1.3 Požadavky na dodávané a stávající SW licence

- V rámci instalace SW ArcSight dojde k migraci stávající licence ArcSight Logger do nové platformy ArcSight Recon, další parametry licencí zůstanou beze změny,
- licence VMware vSphere Essential Kit, který bude nainstalovaný na dodaných serverech,
- licence operačního systému podporovaného výrobcem dodávaného SW ArcSight pro všechny potřebné virtuální servery,
- rozšíření stávající licence o 5000 EPS - licence SW ArcSight Recon,
- rozšíření stávající licence o 500 EPS - licence SW ArcSight ESM,
- nová licence pro 500 entit – licence SW ArcSight Intelligence,
- podpora dodaných SW licencí i stávajících licencí Arcsight,
- podpora stávajících licencí musí být sjenocená s podporou dodaných licencí.

Příloha č. 3

CENOVÁ TABULKA

Dodávka HW a migrace systému SIEM ArcSight, včetně rozšíření licence

Komponenta	Název komponenty	Počet ks	Jednotková cena v Kč bez DPH	Celková cena v Kč bez DPH
Dodávka technických prostředků pro SIEM (dle čl. I odst.1 smlouvy)				
server 1		1	401 603,00	401 603,00
server 2		1	401 603,00	401 603,00
HW pro cold storage, včetně požadované úložné kapacity		1	323 971,00	323 971,00
Dodávka programových prostředků pro SIEM včetně licencí (dle čl. I odst.1 smlouvy)				
Licence podporovaného operačního systému na fyzických i virtuálních serverech		2	272 720,00	545 440,00
Licence VMWare vSphere Essentials plus Kit		1	22 740,00	22 740,00
Rozšíření licence ArcSight Logger o 5000 EPS		1	1 367 444,00	1 367 444,00
Rozšíření licence ArcSight ESM o 500 EPS		1	1 062 503,00	1 062 503,00
Licence ArcSight Intelligence, 500 Entit		1	1 104 320,00	1 104 320,00
Migrace systému SIEM do nové architektury (dle čl. II odst.1 smlouvy)		1	2 275 910,00	2 275 910,00
Zaškolení administrátorů (pracovníků objednatele) dle čl. II odst. 1 písm. b) smlouvy		1	51 050,00	51 050,00

		Cena v Kč za 1 rok bez DPH
Podpora dodaného HW [dle čl. VI odst.1 a) smlouvy]		0,00
Podpora dodaného SW [dle čl. VI odst.1 b) smlouvy]		1 293 682,00
Podpora stávajícího SW (ESM-1000 EPS, Logger 925 EPS)		1 029 582,00

Podpora dle čl. VI odst.1 c) smlouvy (paušální cena)	Počet člověkodnů ročně	Cena za 1 člověkoden v Kč bez DPH	Celková cena v Kč bez DPH za 1 roky
Paušální cena podpory na místě	12	20 000,00	240 000,00

Podpora dle čl. VI odst.1 c) smlouvy (cena nad paušální cenu)	Cena za 1 hodinu v Kč bez DPH
Podpora na místě nad 12 člověkodnů	2 500,00

Celková cena díla v Kč bez DPH	**7 556 584,00**

Příloha č. 4

Bezpečnostní požadavky objednatele

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze ti jeho pracovníci, kteří jsou jmenovitě uvedeni v seznamu pracovníků schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Poskytovatel předloží seznam ČNB nejpozději pět pracovních dní před zahájením prací.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti každého z pracovníků poskytovatele. Poskytovatel se zavazuje zajistit, aby všichni jeho pracovníci uvedení v seznamu byli ještě před předložením seznamu ČNB proškoleni o podmínkách zpracování osobních údajů a o právech subjektů údajů ve smyslu obecného nařízení o ochraně osobních údajů - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“). Poskytovatel se zejména zavazuje, že všichni jeho pracovníci uvedení v seznamu budou nejpozději do okamžiku předložení seznamu ČNB poučeni:
   a) o tom, že poskytovatel předá jejich osobní údaje v rozsahu: jméno, příjmení a číslo průkazu totožnosti České národní bance, sídlem Na Příkopě 28, Praha 1 v rámci plnění této smlouvy, a to za účelem ochrany práv a oprávněných zájmů ČNB (zajištění evidence osob vstupujících do budovy ČNB z důvodu ochrany majetku a osob a správy systému kontrol vstupů ČNB);
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči poskytovateli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovávány, právu na námitku proti zpracování osobních údajů, právu požadovat nápravu situace, která je v rozporu s právními předpisy, a to zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním, jakož i o právu podat stížnost k Úřadu pro ochranu osobních údajů.
3. Za poučení svých pracovníků ponese poskytovatel vůči ČNB následně odpovědnost. V případě nesplnění povinnosti podle odst. 2 této přílohy nahradí poskytovatel újmu, která v souvislosti s uvedeným ČNB vznikne, a to včetně případné nemajetkové újmy vzniklé poškozením dobrého jména a dobré pověsti, újmy vzniklé v důsledku postihu pravomocně uloženého ČNB správním nebo jiným k tomu oprávněným orgánem veřejné moci a újmy vzniklé ČNB v důsledku úspěšného uplatnění práv pracovníků poskytovatele vůči ČNB.
4. Požadavky na případné doplňky a změny schváleného seznamu je nutno neprodleně oznámit ČNB. Případné doplňky a změny seznamu podléhají schválení ČNB. Osoby neschválené ze strany ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Poskytovatel uvede předem ty své pracovníky, pro které požaduje vystavení vstupních karet ke vstupu do objektů ČNB. Vystavení vstupních karet podléhá schválení ze strany ČNB. První vstupní karty budou vystaveny na náklady ČNB. Každé další vystavení vstupní karty bude zpoplatněno částkou 200,- Kč (vč. DPH) s tím, že tato částka bude poskytovateli vyfakturována. Za vystavení nové vstupní karty nebude nutné platit v případech, kdy:
   - dosavadní karta přestane fungovat bez viditelného mechanického poškození,
   - dojde ke změně příjmení pracovníka,

- byla karta odcizena a událost je doložitelná protokolem od Policie ČR.

6. Poskytovatel bude při zahájení činnosti pro ČNB vybaven základním počtem vstupních karet pro jednotlivé pracovníky podle schváleného seznamu. Vstupní karta umožní oprávněnému pracovníkovi poskytovatele samostatný vstup do vyhrazených prostor objektu ČNB a samostatný pohyb v nich. Každá vstupní karta bude nepřenosná a bude vydávána odborem bankovní bezpečnosti a krizového řízení ČNB.
7. Vstupní karty budou vydávány ze strany ČNB pro každého pracovníka poskytovatele jednotlivě proti podpisu, a to po předložení výpisu z rejstříku trestů, který nebude starší než tři měsíce. Výpis z rejstříku trestů bude pracovníkovi vrácen. Při převzetí vstupní karty bude dotčený pracovník poskytovatele poučen o způsobu používání vstupní karty a o režimu vstupu osob a vjezdu vozidel do objektů ČNB a o pohybu v nich.
8. Pracovník poskytovatele, kterému byla vydána vstupní karta, je povinen okamžitě po zjištění ztráty, odcizení, zneužití, zničení nebo poškození vstupní karty, které brání jejímu řádnému užívání, toto oznámit odboru bankovní bezpečnosti a krizového řízení ČNB.
9. Při ukončení pracovního poměru pracovníka poskytovatele uvedeného v seznamu nebo při ukončení plnění podle smlouvy je poskytovatel povinen neprodleně vrátit vstupní kartu dotčeného pracovníka odboru bankovní bezpečnosti a krizového řízení ČNB.
10. ČNB si vyhrazuje právo nevydat vstupní karty pracovníkům poskytovatele bez udání důvodu.
11. ČNB si vyhrazuje právo vstupní kartu pracovníkovi poskytovatele odebrat z důvodu porušení režimu vstupu osob a vjezdu vozidel do objektu ČNB nebo porušení režimu pohybu v něm.
12. ČNB si vyhrazuje právo vyřadit i schválené pracovníky poskytovatele ze seznamu bez udání důvodů. Schválení pracovníci musí dodržovat směrnice ČNB a pokyny ostrahy pro vstup do vyhrazených prostor a pro pobyt v nich.
13. Pracovníci poskytovatele jsou povinni podrobit se při každém vstupu do objektu ČNB bezpečnostní kontrole prováděné bankovními policisty.
14. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
15. Vstup do objektů ČNB se zvířaty je zakázán.
16. Vstup soukromých návštěv do vnitřních prostor objektů ČNB je zakázán. Pro tyto účely je možné využít určené návštěvní místnosti.
17. Poskytovatel je povinen zajistit, že jeho pracovníci budou vstupovat do prostorů ČNB a zdržovat se v nich pouze ve firemním pracovním oděvu s viditelným nesnímatelným označením logem poskytovatele. Pracovní oděv musí být doplněn viditelně nošenou vstupní kartou vydanou ČNB každému pracovníkovi poskytovatele podle schváleného seznamu.
18. Poskytovatel a jeho pracovníci budou věnovat při plnění díla v oblasti požární ochrany zvýšenou pozornost:
    - dodržování právních předpisů o požární ochraně,
    - předpisům ČNB při provádění požárně nebezpečných prací se zvýšeným požárním nebezpečím (svařování, řezání plamenem, pájení, broušení, rozbrušování apod.),

- průrazům a průchodům u rozvodů instalací a technologií hranicemi požárních úseků, včetně zachování, obnovení nebo nového vyhotovení jejich protipožárních ucpávek.

19. Poskytovatel se zavazuje zajistit, že jeho pracovníci, jakož i pracovníci případných jeho poddodavatelů, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se v průběhu plnění seznámí a které nejsou veřejně známy.
20. Povinnost mlčenlivosti podle odst. 19 této přílohy není časově omezena.
21. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem ČNB.
22. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny, hořlavé kapaliny, tlakové lahve apod. O tom, co je či není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
23. Fotografování a pořizování videozáznamů je ve všech prostorách objektů ČNB zakázáno. Výjimku tvoří pořizování dokumentace technických havárií a poruch. Konkrétní případ musí předem písemně povolit ředitel odboru bankovní bezpečnosti a krizového řízení nebo ředitel příslušné pobočky ČNB.
24. Ve všech prostorách objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení k provedení požárně nebezpečné práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou dozorujícího zaměstnance ČNB, a to vždy nejpozději jeden pracovní den před zahájením prací.
25. Pracovníci poskytovatele se musí zdržet poškozování či odcizení majetku ČNB, a dále i jakéhokoli nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
26. Pracovníci poskytovatele uvedení na seznamu se musí před započetím výkonu práce v objektech ČNB prokazatelně seznámit s „Pravidly pro smluvní partnery ČNB k zajištění bezpečnosti a ochrany zdraví při práci, požární ochrany a ochrany životního prostředí v ČNB“ (dále jen „pravidla“). Pravidla předá v listinné formě zástupci poskytovatele požární a bezpečnostní technik ČNB. Zástupce poskytovatele s pravidly seznámí všechny dotčené pracovníky poskytovatele.
27. ČNB je oprávněna v objektu ČNB kdykoliv podrobit kontrole kteréhokoliv pracovníka poskytovatele uvedeného na seznamu ohledně dodržování požární ochrany, bezpečnosti práce a všech výše uvedených ustanovení.

Příloha č. 5

Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu této smlouvy nebo zadávací dokumentace nebo její jinou přílohou, má přednost ustanovení textu této smlouvy nebo zadávací dokumentace nebo její jiná příloha.
2) Poskytovatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
3) Poskytovatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy s ČNB.
4) Poskytovatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
5) Pracovníci poskytovatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
6) Poskytovatel a jeho pracovníci nejsou oprávněni:
   a) obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
   b) sdělovat své přístupové údaje k systémům ČNB;
   c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
   d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
7) Poskytovatel a jeho pracovníci jsou povinni:
   a) okamžitě nahlásit sekci informatiky, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro poskytovatele a uživatele, jejichž předmět smlouvy nebo pracovní náplň obsahuje tuto činnost;
   b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit a ověřit, že k odhlášení/uzamčení opravdu došlo;
   c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku;
   d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
   e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku.

8) Pracovníci poskytovatele nesmí:
   a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);
   b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).
9) Poskytovatel a jeho pracovníci nejsou oprávněni:
   a) používat soukromou e-mailovou schránku pro činnosti související s plněním dle této smlouvy, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;
   b) nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;
   c) ukládat jiné než veřejné informace mimo úložiště pod správou ČNB (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).
10) Poskytovatel a jeho pracovníci nejsou oprávněni:
   a) nepovoleně používat, kopírovat a šířit software, jako např.:
      i) instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);
      ii) instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět této smlouvy obsahuje tuto činnost;
      iii) instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí
         (1) pro situace výslovně schválené a popsané v jiném vnitřním předpisu (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a
         (2) v případech, kdy předmět této smlouvy obsahuje tuto činnost;
   b) používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;
   c) bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

1) Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.
2) Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů na Internet automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).