

SMLOUVA O POSKYTOVÁNÍ KONZULTAČNÍCH SLUŽEB

Č. j. MV-158984-3/SIK5-2022

Česká republika – Ministerstvo vnitra

Se sídlem: Nad Štolou 936/3, 170 34 Praha 7

Zastoupená: Mgr. Bohdanem Urbanem, ředitelem odboru provozu informačních
technologií a komunikací

Kontaktní adresa: Nagano III, U Nákladového nádraží 3265/10, 130 00 Praha 3

IČO: 00007064

DIČ: CZ00007064

Bankovní spojení: ČNB Praha 1

Číslo účtu: 3605881/0710

(dále také jen „**Klient**“)

a

Crayon Czech Republic and Slovakia s.r.o.

Se sídlem: Evropská 2591/33d, Dejvice, 160 00 Praha 6

Zastoupená: Dr. Ing. Miroslavem Holušou

IČ: 08555532

DIČ: CZ08555532

Bankovní spojení: BNP Paribas S.A., pobočka Česká republika

Číslo účtu: 064450-6006140001/6300

vedená u Městského soudu v Praze, C 320900

(dále také jen „**Konzultant**“)

(Konzultant a Klient dále společně také jen „**Smluvní strany**“)

uzavírají podle § 1746 zákona č. 89/2012 Sb., občanský zákoník tuto Smlouvu o poskytování konzultačních služeb (dále také jen „**Smlouva**“):

I.

Předmět Smlouvy

1. Předmětem této Smlouvy je poskytování konzultačních služeb ve vybraných oblastech kybernetické bezpečnosti a řešení EDR (Endpoint Detection and Response) od společnosti Microsoft v prostředí Klienta.
2. Konzultant se zavazuje poskytovat Klientovi konzultační služby za účelem zvýšení kybernetické bezpečnosti v oblasti provozu informačních technologií. Dále pak konzultační služby při zajištění lepší kontroly a správy koncových zařízení. Výstupem plnění bude dodržení Zákona o kybernetické bezpečnosti a schopnost reagovat na některé specifické doporučení Národního úřadu pro kybernetickou a informační bezpečnost. Podrobnější specifikace předmětu plnění je uvedena v Příloze č. 1 smlouvy.
3. Konzultant se touto Smlouvou zavazuje poskytovat konzultační služby v celkovém rozsahu 20,5 MD's. Předpokládané poskytnuté role – Security Architekt EDR (Microsoft EDR technologie) a Cyber Security Consultant.
4. Konzultant bude konzultační služby poskytovat na základě Klientova příkazu nebo zadání, ze kterého bude vyplývat požadovaná služba.

II.

Práva a povinnosti Smluvních stran

1. Konzultant se zavazuje postupovat při vyřizování všech záležitostí pro Klienta s odbornou péčí a v souladu s pokyny Klienta, zároveň se zavazuje oznámit Klientovi všechny okolnosti, které zjistil při poskytování konzultačních služeb, a jež mohou mít vliv na změnu jeho pokynů.
2. Konzultant však není vázán pokyny Klienta, jsou-li v rozporu se zákonem nebo se stavovskými předpisy.
3. Klient se zavazuje poskytovat Konzultantovi včasné, pravdivé, úplné a přehledné informace. Klient je povinen informovat včas Konzultanta o skutečnostech důležitých pro řádné vykonávání jemu svěřených záležitostí a předat mu včas a řádně veškeré potřebné podklady.
4. Konzultant se zavazuje zachovávat mlčenlivost v rozsahu svěřených záležitostí.

III.

Smluvní odměna

1. Smluvní odměna bude hrazena na základě počtu člověkodní, přičemž odměna za jeden (1) člověkodnen je 14.500,00 Kč (slovy: čtrnáct tisíc pět set korun českých) bez DPH, samostatně příslušná sazba DPH 3.045,00 Kč, tj. 17.545,00 Kč (slovy: sedmnáct tisíc pět set čtyřicet pět korun českých) včetně DPH.
2. Smluvní strany se dohodly, že celková cena za Konzultantem poskytnuté služby dle této Smlouvy nepřekročí 297.250,00 Kč (slovy: dvě stě devadesát sedm tisíc dvě stě padesát korun českých) bez DPH, tj. **359.672,50 Kč** (slovy: tři sta padesát devět tisíc šest set sedmdesát dva korun českých padesát haléřů) **včetně DPH.**

3. Odměna bude splatná měsíčně pozadu v českých korunách, a to do 30 dnů ode dne vystavení faktury na bankovní účet Konzultanta vyznačený na faktuře. Přílohou faktury bude přehled poskytnutých konzultačních služeb s časovou specifikací.
4. Běžné administrativní náklady Konzultanta, tj. např. poštovné, náklady kancelářských potřeb, kopírování, telekomunikace apod., jsou zahrnuty v jeho odměně.
5. Klient se zavazuje zaplatit odměnu Konzultanta dle tohoto článku Smlouvy na bankovní účet vedený u BNP Paribas S.A., pobočka Česká republika, č. ú. 064450-6006140001/6300.

IV.

Platnost Smlouvy

1. Smlouva se uzavírá na dobu určitou, a to do **15. 12. 2022** nebo do vyčerpání maximální smluvní částky dle čl. III. Odst. 2. Smlouvy.
2. Prodlení Klienta s úhradou odměny za poskytované konzultační služby přesahující jeden měsíc je důvodem k okamžitému odstoupení od této Smlouvy Konzultantem.
3. Klient je oprávněn od Smlouvy odstoupit v případě, že Konzultant hrubě poruší své povinnosti vyplývající pro něj z této Smlouvy.
4. Odstoupení od Smlouvy Konzultantem či Klientem je účinné doručením písemného odstoupení druhé Smluvní straně.

V.

Závěrečná ustanovení

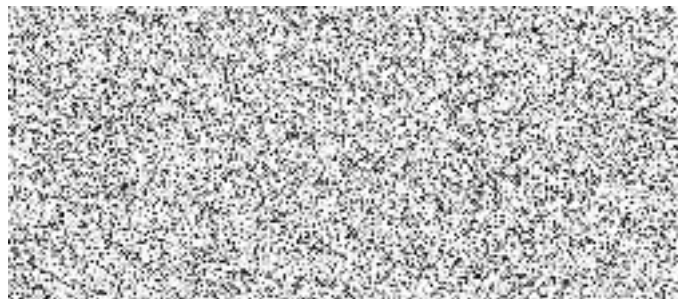
1. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv.
2. Tato Smlouva se vyhotovuje výhradně elektronicky.
3. Tato Smlouva může být měněna a doplňována pouze písemným dodatkem.
4. Obě Smluvní strany souhlasně prohlašují, že si tuto Smlouvu důkladně přečetly a s jejím obsahem souhlasí, a že Smlouvu uzavřely dobrovolně a nikoliv v tísní ani za nápadně nevýhodných podmínek, vědomy si svých práv a závazků z ní vyplývajících, na důkaz čehož zdola připojují své podpisy.

V _____ dne _____

V _____ dne _____

Mgr. Bohdan Urban, ředitel

Dr. Ing. Miroslav Holuša, jednatel



Příloha č. 1 smlouvy č.j. MV-158984-3/SIK5-2022

1.) EDR Popis oblasti řešení (Endpoint Detection and Response)

- Analýza stávajícího stavu
- PoC a doporučení nastavení dle požadavku zákazníka
- Předání Výsledku s vazbou na ZKB, Security Configuration Framework

Obsahem je:

- Antivirus
- Antimalware
- Vulnerability scanner
- Web filtering
- Inventory
- Hunting/Investigation
- Threat analytics
- Konfigurace a implementace
- Silné a slabé stránky v porovnání ke stávajícímu řešení zákazníka
- Hybridní mód a porovnání se stávajícím Antimalware řešením
 - Nálezy ohrožení
- Identifikace důležitých nálezů a reportů
- SW inventory koncových zařízení
- Functionality s vazbou na Exchange Online (EOP) Hybridní mód
- Security skóre
- Vizualizace informací:
 - Alarmy & Bezpečnostní incidenty
 - Řízení zranitelností (Vulnerability management)
 - Exposure score
 - Security doporučení

 - Slabé stránky
 - Časová osa
 - Reportování zranitelností (Vulnerability reports)

Popis Pilotního Projektu EDR - (50 – 3000 uživatelů)

PoC for Azure Defender for server and Defender for endpoint Plan 1 and Plan 2 (formaly Defender for Endpoint)

- Strategic goal is to present strengths of security products and optionally compare them with actual products. To show installation, configuration and deployment training for users end points and servers.

1st phase: Installation and configuration of Defender for Endpoint Plan 1 and Plan 2

End users except “temporary ones” VDI

- Windows - GPO (InTune?)

- Apple (MacOS)

Mobile devices (Optional)

-Android

-iOS

Required cooperation:

- Understand business needs and strategic security goals of company
- Understanding of Priority
- Very close cooperation with customer due to internal infrastructure rules and Configuration

Required cooperation:

- Guarantee availability of key persons
- Global Admin permission required (or remote dual remote cooperation)
- 1:1 More Config sessions

Expected output:

- Ready to run Pilot with Defender for Endpoint Plan2
- Receive trial licences from Microsoft

2nd phase: Setup scenarios to run Pilot and collect data and information from all end users stations and optionally set up Hybrid mode to compare result (Vulnerability findings) with current Antimalware

- Extensive weekly regularly based 1:1 activity to check and understand information and outputs receiving continuously
- Optionally configure Hybrid mode with current Antimalware to see delta and different with Vulnerability findings
- Very intensive close cooperation and practical training phase for 4 weeks
- Identify important findings, reports
- Optionally to demonstrate strengths of SW inventory of endusers
- Functionalities in connection to Exchange Online
- Understand security scores development and consequences during PoC
- Understanding of visible information
- Detailed differentiator between P1 and P2

Required cooperation:

- Guarantee availability of key persons
- 1:1 intensive cooperation required
- Whole scope and deep dive will be based on commitment and preferences from customer
- This phase required biggest effort on customer side

expected output:

- Data for PoC result and findings collected
- What is visible, what you want to see and how to get there
- Ready to show scenarios and be ready for output

3rd phase: PoC result presentation and demonstration

- Final project result presentation
- Alerts & Incidents
- Vulnerability management
- Exposure score
- Security recommendations
- Weaknesses
- Event timeline
- Vulnerability reports
- Optional Delta Comparison with current Antimalware
- Optional Delta Comparison with current EDR
- Next steps discussion and scenariouse

- o SW and Patch Inventory Dashboards (optional Vulnerability mng. Add-on)
 - o Pilot project deinstallation
 - o Switch EDR Project into production
- o deployment plan for end users (can be done during Pilot)

2.) Další konzultační služby

- o Forensní investigace incidentů (L3)
- o Podpora L2
- o Audit Password Policy
- o Bezpečnostní rating společností a institucí (Microsoft technologií)
- o Licenční podpora a nákladová optimalizace, Business case
 - o Nastavení parametrů a doporučení
- o Podpora po instalaci Microsoft produktů
 - o Po aktivaci Microsoft produktů nabízíme 1x týdně 2 hodinovou konzultaci po dobu x týdnů dle požadavků zákazníka
- o Návrh Metodologie (Feasibility study) – služby „Preventivní kontrola rizik a zranitelnosti společností a institucí – Proaktivním způsobem“

