Smlouva o implementaci SW nástroje pro skenování zranitelností a o poskytování služeb podpory

č. UKRUK/511236/2023

(dále jen „Smlouva“)

Smluvní strany:

Univerzita Karlova

se sídlem: Ovocný trh 560/5, 116 36 Praha 1,
zastoupená: Mgr. Martinem Maňáskem, kvestorem
IČO: 00216208, DIČ: CZ00216208
bank. spojení: [redacted]
ID datové schránky: piyj9b4
(dále jen „kupující“)

a

Security Avengers s.r.o.

se sídlem: Kaprova 42/14, Staré Město, 110 00 Praha 1
registrovaný: Spisová značka C 339054 vedená u Městského soudu v Praze
zastoupený: Ing. Matej Kačic, Ph.D., jednatel
IČO: 09617477, DIČ: CZ09617477
tel.: [redacted]
bank. spojení: [redacted]
ID datové schránky: 88kn9d8
(dále jen „prodávající“)
(dále společně kupující a prodávající jako „smluvní strany“)

uzavírají v souladu s ustanoveními § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník“) tuto Smlouvu:

1. Úvodní prohlášení

1.1. Univerzita Karlova (dále též „UK“), v souladu se zákonem č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, v platném znění (zákon o vysokých školách), jako kupující prohlašuje, že je oprávněna uzavřít a řádně plnit tuto Smlouvu a závazky v ní obsažené.

1.2. Společnost Security Avengers s.r.o. jako prodávající prohlašuje, že je právnickou osobou řádně založenou a zapsanou podle českého právního řádu v obchodním rejstříku vedeném Městským soudem v Praze oddíl C vložka 339054, a že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.3. Prodávající bere na vědomí, že plnění, které je předmětem této smlouvy (dodávka) je realizováno v rámci projektu kupujícího s názvem „Digitalizace vzdělávací činnosti a studijních agend“, reg. č: NPO_UK_MSMT-16602/2022, A1 (dále jen „Projekt“). Projekt je realizován v rámci Národního plánu obnovy, jehož řídícím orgánem je Ministerstvo školství, mládeže a tělovýchovy České republiky (dále rovněž jen „MŠMT“) a který je spolufinancován z Evropského fondu pro regionální rozvoj a ze státního rozpočtu České republiky. Poskytovatelem dotace je Česká republika prostřednictvím MŠMT. Z tohoto důvodu se na plnění této smlouvy a na následnou kontrolu vztahují mimo Zákon i další právní předpisy (např. zák. č. 320/2001 Sb., o finanční kontrole ve veřejné správě, zák. č. 255/2012 Sb., o kontrole (dále jen „kontrolní řád“), ve znění pozdějších předpisů, a zák. č. 130/2002 Sb. o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů) a Rozhodnutí MŠMT o poskytnutí dotace.

1.4. Prodávající se zavazuje, že poskytne součinnost při kontrolách subjektům, které jsou oprávněny ke kontrole dotačních prostředků

1.5. Prodávající prohlašuje, že on sám i jeho případný poddodavatel (poddodavatelé) není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 sb., o střetu zájmů nebo, jím ovládaná osoba, vlastní podíl představující alespoň 25% účasti společníka v obchodní společnosti. Prodávající prohlašuje, že se na nabízené plnění nevztahují sankce EU a že on ani jeho poddodavatel (poddodavatelé) není osobou, subjektem či orgánem uvedeným na sankčním seznamu EU, nebo osobu, subjektem či orgánem, na které se vztahuje zákaz zadat nebo dále plnit veřejnou zakázku (čl.5k Nařízení Rady (EU) č. 2022/576 ze dne 8.4.2022, kterým se mění Nařízení (EU) č. 833/2014, o omezujících opatřeních vzhledem k činnostem Ruska, destabilizujícím situaci na Ukrajině).

2. Východiska a účel Smlouvy

2.1. Kupující provedl v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“) řízení na zadání veřejné zakázky malého rozsahu s názvem „*RUK – ÚVT – Sken zranitelností*".

2.2. Nabídka prodávajícího byla v řízení na základě stanovených hodnotících kritérií vybrána jako ekonomicky nejvýhodnější.

2.3. Záměrem kupujícího je získat oprávnění k užití softwarového produktu skenu zranitelností, jeho implementaci včetně procesu řízení technických zranitelností a poskytnutí související podpory, jak je dále uvedeno v této Smlouvě.

3. Předmět smlouvy, termíny a místo plnění

3.1. Předmět této Smlouvy detailně upravuje Příloha č. 1 – Specifikace a rozsah předmětu plnění. Předmět této Smlouvy zahrnuje mimo jiné:

a) Závazek prodávajícího poskytnout oprávnění k užití softwarového produktu skenu zranitelností dle Přílohy č. 1 této smlouvy (dále také „**VMS**“).

b) Závazek prodávajícího zajistit implementaci software VMS, zpracování dokumentace skutečného provedení, vytvoření, zavedení a optimalizaci procesu řízení technických zranitelností.

3.2. Předmětem této smlouvy je taktéž zajištění správy a provozní podpory řešení skenu zranitelností v prostředí kupujícího (dále jen „**provozní podpora**“), a to v souladu s článkem 4 této Smlouvy po dobu uvedenou v čl. 3.4. této Smlouvy.

3.3. Kupující se zavazuje zaplatit prodávajícímu cenu v souladu s článkem 7 a přílohou č. 2 této Smlouvy, odpovídající nabídkové ceně v zadávacím řízení.

3.4. Službu provozní podpory uvedenou v čl. 3.2. a dále v článku 4 Smlouvy se prodávající zavazuje poskytovat průběžně od nasazení VMS do produkčního prostředí Kupujícího do 30.6.2024.

3.5. Místem plnění je pracoviště ÚVT Ovocný trh 650/5, Praha 1.

4. Poskytování provozní podpory

4.1. Prodávající se zavazuje k zajištění provozní podpory řešení VMS v rozsahu:

a) profylaktické činnosti, kontrola služeb (1x měsíčně),

b) kontrola provozních logů zařízení (1x měsíčně),

c) návrh případných opatření s cílem předejít možným výpadkům a omezením poskytovaných služeb řešením VMS (dle potřeby, min. 1x měsíčně),

d) odborná technická podpora a odstraňování závad v předmětné oblasti (průběžně),

e) kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce (denně),

f) údržba a zajištění dostupnosti služby VMS (98% za kalendářní měsíc),

g) analýza vhodnosti a potřebnosti implementace opravného balíku (pravidelně při vydání opravného balíku),

h) návrh opatření a postupu implementace opravného balíku ke schválení kupujícímu (pravidelně při vydání opravného balíku),

4.2. Ostatní činnosti, které jsou předmětem provozní podpory:

a) zajištění telefonické podpory pro konzultaci problematiky řešení VMS v provozním režimu 5x8 (v pracovní dny minimálně od 8 do 16:30 hod) na tel. lince [redacted]

4.3. Prodávající se zavazuje výše uvedené činnosti vykonávat s odbornou péčí dostatečně kvalifikovanými pracovníky, kteří jsou certifikováni k provádění implementace a technické podpory kupujícím používaného řešení VMS. Tito pracovníci jsou jmenovitě uvedeni v příloze č. 3 této Smlouvy, která je nedílnou součástí Smlouvy. Nahrazení pracovníka uvedeného v příloze č. 3 této Smlouvy jinou osobou nevyžaduje uzavření dodatku k této Smlouvě, prodávající je však povinen takovou změnu

kupujícímu písemně oznámit minimálně 2 pracovní dny před zapojením takové jiné osoby do plnění předmětu Smlouvy. Smluvní strany z důvodu právní jistoty sjednávají, že i na tuto jinou osobu se aplikuje věta první tohoto článku Smlouvy.

5. Práva a povinnosti smluvních stran

5.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků.

5.2. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob uvedených v Příloze č. 3 Smlouvy – Seznam oprávněných osob.

5.3. Obě strany vyvinou maximální úsilí pro zajištění ochrany informací, které v rámci plnění této smlouvy získá jedna strana od druhé.

5.4. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů a k jejich vyřešení zejména prostřednictvím jednání oprávněných osob nebo statutárních zástupců smluvních stran. Nedojde-li k dohodě, je každá smluvní strana oprávněna předat spor místně a věcně příslušnému soudu. Rozhodčí řízení je vyloučené.

5.5. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.

5.6. Smluvní strany jsou povinny plnit své závazky vyplývající z této smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a splatností jednotlivých peněžních závazků.

6. Předání a převzetí předmětu plnění

6.1. Dodání plnění dle čl. 3.1 této Smlouvy bude probíhat na základě schváleného harmonogramu implementace (Solution design).

6.2. Převzetí předmětu plnění dle čl. 3.1 této Smlouvy kupujícím proběhne na základě akceptace splnění požadavků na implementaci díla dle požadavků definovaných v Příloze č. 1 toto Smlouvy (Požadavky na implementaci díla).

6.3. Při dodání předmětu plnění dle čl. 3.1. této Smlouvy kupujícímu bude mezi prodávajícím a kupujícím podepsán předávací protokol.

7. Kupní cena a platební podmínky

7.1. Cena za předmět smlouvy dle čl. 3.1. a 3.2. Smlouvy bude odpovídat cenám uvedeným v Příloze č. 2 této smlouvy (Položkový rozpočet).

7.2. Kupní cena za VMS stanovená v Příloze č. 2 této Smlouvy je stanovena jako nejvýše přípustná, přičemž zvýšení této ceny je přípustné pouze v souvislosti se změnou výše DPH.

7.3. Cenu za plnění dle čl. 3.1. Smlouvy bude prodávající fakturovat a fakturu doručí kupujícímu po podepsání předávacího protokolu dle čl. 6.3. Přílohou faktury bude předávací protokol podepsaný oprávněnými osobami za obě smluvní strany.

7.4. Datem uskutečnění zdanitelného plnění je datum podpisu předávacího protokolu dle čl. 6.3. smlouvy.

7.5. Cena za služby podpory dle článku 4 této Smlouvy bude kupujícím hrazena jednorázově za poskytované služby podpory, a to na základě daňového dokladu vystaveného prodávajícím.

7.6. Daňové doklady (faktury) budou vystaveny do patnácti (15) kalendářních dnů po uskutečnění zdanitelného plnění nebo po ukončení kalendářního měsíce (v závislosti na fakturovaném plnění).

7.7. Faktura vystavená prodávajícím dle této Smlouvy bude vystavena jako daňový doklad se zúčtováním DPH podle předpisů platných k datu zdanitelného plnění a musí mít náležitosti stanovené příslušnými právními předpisy pro daňový doklad. Splatnost faktury bude třicet (30) kalendářních dnů od prokazatelného doručení faktury kupujícímu. Dnem uhrazení faktury je den, kdy byla příslušná částka odepsána z účtu kupujícího ve prospěch účtu prodávajícího.

7.8. Faktura prodávajícího musí být vystavena v souladu s touto Smlouvou a musí mít náležitosti daňového dokladu dle zákona č. 235/2004 Sb., ve znění pozdějších předpisů, zejména:

a) evidenční číslo daňového dokladu,
b) název a sídlo kupujícího a prodávajícího,
c) číslo Smlouvy a den jejího uzavření,
d) název projektu: Transformace pro VŠ na UK, registrační číslo: NPO_UK_MSMT-16602/2022, SC A1,
e) datum vystavení daňového dokladu a datum uskutečnění zdanitelného plnění,
f) označení banky a číslo účtu, na který má být zaplaceno a který je registrován u příslušného správce daně a je zveřejněn způsobem umožňujícím dálkový přístup ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění,
g) předmět plnění,
h) jednotkovou cenu bez daně a slevu, není-li obsažena v jednotkové ceně, základ daně, sazbu daně a její výše, pokud nejde o plnění dle ust. § 92e zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění,
i) číselný kód klasifikace CPV, a v případě plnění dle ust. § 92e zákona o DPH poznámku „daň odvede zákazník“,
j) čísla a data vyhotovení soupisů skutečně a řádně provedených prací a zjišťovacích protokolů,
k) IČO a DIČ prodávajícího a kupujícího,
l) podpis oprávněné osoby za prodávajícího,
m) příloha faktury:

7.9. předávací protokol potvrzený oprávněnou osobou kupujícího. Kupující se zavazuje proplatit v termínu fakturu vystavenou prodávajícím v souladu s ustanovením čl. 7 této Smlouvy. Nesprávně nebo neúplně vyplněnou fakturu je kupující oprávněn vrátit prodávajícímu k opravě, po tuto dobu neběží doba splatnosti faktury. Po prokazatelném doručení bezchybné faktury kupujícímu počíná běžet nová lhůta splatnosti.

7.10. V případě, že se prodávající stane nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, je povinen o tom neprodleně písemně informovat kupujícího. Bude-li prodávající ke dni uskutečnění zdanitelného plnění veden jako nespolehlivý plátce, bude část ceny za služby dle této Smlouvy odpovídající dani z přidané hodnoty uhrazena přímo na účet správce daně v souladu s ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. O tuto částku bude ponížena celková cena a prodávající obdrží cenu dle této Smlouvy bez DPH. V případě, že se prodávající stane nespolehlivým plátcem ve smyslu tohoto článku 7.10, má kupující současně právo od této smlouvy odstoupit.

8. Sankce

8.1. V případě prodlení Prodávajícího s poskytnutím plnění dle čl. 3.1 či stanovených dílčích milníků v termínu dle Smlouvy nebo na základě harmonogramu plnění je Prodávající povinen uhradit Kupujícímu smluvní pokutu ve výši 10.000 Kč, a to za každý i započatý den prodlení a za každé jednotlivé porušení.

8.2. V případě porušení poskytování služeb podpory dle čl. 4 Smlouvy je Prodávající povinen uhradit Kupujícímu smluvní pokutu ve výši 1.000 Kč za každé takové porušení.

8.3. V případě porušení povinností k ochraně důvěrných informací dle článku 12. Smlouvy je Prodávající povinen uhradit Kupujícímu smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ porušení.

9. Řádné plnění

9.1. Prodávající odpovídá za porušení práv duševního vlastnictví třetích osob v souvislosti s plněním svých povinnosti dle předmětu této Smlouvy.

9.2. Prodávající odpovídá za právní vady plnění podle této smlouvy.

9.3. Prodávající se zavazuje, že při plnění této smlouvy nepoškodí práva třetích osob.

10. Řešení sporů

10.1. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou a k jejich vyřešení zejména prostřednictvím jednání zplnomocněných zástupců dle čl. 5.2. této smlouvy.

10.2. Jestliže se spory nepodaří vyřešit smírnou cestou, může každá ze stran postoupit spor nejvyšším představitelům smluvních stran. Nejvyšší představitelé se pokusí vyřešit spor smírnou cestou. Případný soudní spor bude řešen věcně a místně příslušným soudem. Rozhodčí řízení se nepřipouští.

11. Ochrana osobních údajů

11.1. Smluvní strany prohlašují, že jsou schopny zajistit technické a organizační zabezpečení ochrany osobních údajů; zejména přijmout veškerá opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, jakož i jejich zneužití, včetně opatření týkajících se práce s informačními systémy, v nichž jsou tyto osobní údaje zpracovávány a zajistit mlčenlivost o údajích, které se v rámci zpracování osobních údajů dozvěděly.

11.2. Smluvní strany se dohodly, že pokud takto získají od druhé smluvní strany informace, bez ohledu na formu jejich zachycení, o kterých mohly při vynaložení veškerého možného úsilí, které lze spravedlivě požadovat, vzhledem k povaze takových informací předpokládat, že na jejich utajení má druhá smluvní strana oprávněný zájem, a které nejsou v obchodních kruzích dostupné a zároveň nejsou některou ze smluvních stran označeny jako veřejné (dále jen „důvěrné informace"), budou s těmito důvěrnými informacemi nakládat jako s vlastním obchodním tajemstvím. Dále se za důvěrné informace považují informace uložené v informačních systémech smluvních stran. Zároveň smluvní strany berou na vědomí, že některé z těchto informací jsou také předmětem obchodního tajemství druhé smluvní strany, chráněným dle příslušných ustanovení občanského zákoníku.

11.3. Pro nakládání s osobními údaji, s nimiž některá ze smluvních stran přijde do styku v průběhu plnění této smlouvy a pro ochranu těchto údajů při jejich zpracování platí v plném rozsahu pro obě smluvní strany ustanovení zákona č. 110/2019 Sb., o zpracování osobních údajů a nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

11.4. Kupující poskytne prodávajícímu pro plnění smlouvy zabezpečený vzdálený přístup k softwarovému řešení skenu zranitelností, který bude provozován u kupujícího. Prodávajícímu bude do skenu zranitelností poskytnut přístup nezbytný k plnění předmětu smlouvy, a to po dobu její platnosti a účinnosti. Prodávající je povinen zajistit, že vzdálený přístup do skenu zranitelností budou mít pouze osoby, které jsou v době trvání smlouvy v pracovněprávním nebo obdobném smluvním vztahu s prodávajícím, podílejí se na plnění předmětu smlouvy a jsou písemně zavázány vůči prodávajícímu povinností mlčenlivosti. Zabezpečený vzdálený přístup do skenu zranitelností bude omezen na vyjmenované pracovníky prodávajícího, kterým bude kupujícím přiděleno přístupové jméno a heslo. Zabezpečený vzdálený přístup bude možný pouze z předem dohodnutých síťových adres a omezen na přístupové protokoly dohodnuté mezi technickými zástupci smluvních stran uvedenými ve smlouvě.

11.5. Povinnost oboustranného utajení důvěrných informací platí bez ohledu na ukončení účinnosti této smlouvy.

11.6. Smluvní strany mají právo požadovat navzájem doložení dostatečnosti utajení důvěrných informací.

11.7. Smluvní strany jsou povinny respektovat veškerá práva a oprávněné zájmy druhé smluvní strany a její obchodní značky, loga a ochranné známky.

11.8. Prodávající se zavazuje, že každou tiskovou zprávu nebo jinou informaci určenou ke zveřejnění a týkající se této smlouvy či průběhu jejího plnění předloží ke schválení a korektuře kupujícímu a nebude ji publikovat bez předchozího písemného schválení kupujícím.

11.9. V případě, že prodávající poruší některé ustanovení uvedené v tomto článku, je povinen uhradit kupujícímu smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení povinnosti uvedené v tomto článku, a to bez ohledu na to, zda kupujícímu porušením povinnosti skutečně újma vznikla. Bez ohledu na uhrazení smluvní pokuty má kupující nárok na náhradu vzniklé škody.

11.10. Žádné ustanovení této smlouvy nebrání žádné ze smluvních stran v poskytnutí informací orgánům státní a veřejné správy České republiky, pokud povinnost poskytnutí těchto informací vyplývá z platných právních předpisů. Prodávající bere na vědomí, že kupující je povinným subjektem ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění, a že je povinen žadatelům poskytovat informace dle tohoto zákona.

12. Ochrana důvěrných informací

12.1. Smluvní strany se dohodly, že veškeré informace, které si sdělily v rámci uzavírání a plnění Smlouvy, dále informace, které si sdělí nebo jinak vyplynou i z jejího plnění, jsou důvěrné (dále jen „*Důvěrné informace*“). Smluvní strany sjednávají, že Důvěrnými informacemi jsou veškeré Kupujícím poskytnuté informace, podklady a dokumenty, pokud nejsou běžně dostupné ve veřejných zdrojích.

12.2. Smluvní strany se dohodly, že Důvěrné informace nikomu neprozradí a přijmou taková opatření, která znemožní jejich přístupnost třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy:

a) Smluvní strany mají povinnost stanovenou právním předpisem, a/nebo

b) takové informace sdělí osobám, které mají ze zákona stanovenou povinnost mlčenlivosti u osob za Kupujícího a/nebo

c) takové informace sdělí osobám, které mají ze zákona stanovenou povinnost mlčenlivosti a současně, kterým je nezbytné poskytnout tyto informace výhradně z důvodu plnění této Smlouvy Prodávajícím (tzn. nikoliv osoby vykonávající advokacii dle zákona o advokacii a jiní poradci Prodávajícího) a/nebo

d) se takové informace stanou veřejně známými či dostupnými jinak než porušením povinností vyplývajících z tohoto článku Smlouvy.

12.3. Vyjma výše uvedeného se Prodávající zavazuje, že bude chránit a utajovat před třetími osobami skutečnosti tvořící obchodní tajemství, Důvěrné informace a jiné skutečnosti, které mu byly poskytnuty v rámci smluvního vztahu s Kupujícím.

12.4. Pokud je sdělení Důvěrných informací třetí osobě nezbytné pro plnění závazků Poskytovatele vyplývajících mu ze Smlouvy, může Prodávající tyto Důvěrné informace poskytnout pouze s předchozím písemným souhlasem Kupujícího a za předpokladu, že tato třetí osoba před započetím činnosti písemně potvrdí svůj závazek zachování mlčenlivosti a ochrany Důvěrných informací, jinak je za toto porušení odpovědný v plném rozsahu Prodávající.

12.5. V případě uplatnění smluvních pokut a náhrady újmy není dotčena hmotná a trestní odpovědnost fyzických osob, které za Prodávajícího jednaly a závazek mlčenlivosti a ochrany Důvěrných informací nedodržely.

12.6. Závazek k mlčenlivosti a ochrany Důvěrnosti informací je platný bez ohledu na ukončení účinnosti Smlouvy.

12.7. Vzhledem k veřejnoprávnímu charakteru Kupujícího Prodávající výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených ve Smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

13. Platnost a účinnost Smlouvy

13.1. Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran, přičemž platí datum pozdějšího podpisu a účinnosti dnem uveřejnění smlouvy v registru smluv.

13.2. Smlouva je uzavřena na dobu určitou a skončí řádným a úplným splněním předmětu této Smlouvy smluvními stranami.

13.3. Tuto smlouvu lze ukončit:

a) dohodou smluvních stran, jejíž součástí bude i vypořádání vzájemných závazků a pohledávek.

b) písemnou výpovědí. Výpovědní doba je tříměsíční a začíná běžet od prvního dne měsíce následujícího po doručení výpovědi druhé smluvní straně. Poskytování služeb končí posledním dnem výpovědní lhůty.

c) odstoupením od smlouvy za podmínek v ní ujednaných a v případě podstatného porušení smluvních závazků jednou smluvní stranou, zejména při prodlení Prodávajícího s implementací VMS do produkčního prostředí Kupujícího v souladu s harmonogramem implementace delším než 30 dnů, dále v případě opakovaného prodlení kupujícího s plněním povinností vyplývajících z této smlouvy.

14. Závěrečná ustanovení

14.1. Práva a povinnosti touto Smlouvou výslovně neupravená se řídí příslušnými ustanoveními občanského zákoníku, autorským zákonem a případně dalšími obecně závaznými právními předpisy dopadajícími na předmět plnění.

14.2. Bude-li některé ustanovení této Smlouvy shledáno jako neplatné nebo nevymahatelné, nemá taková skutečnost vliv na platnost nebo vymahatelnost zbývajících ustanovení této Smlouvy.

14.3. Jestliže smluvní strana v případě neplnění či porušení této Smlouvy neuplatní všechna svá práva v takovém případě jí náležející, nelze takové jednání v žádném případě vykládat jako vzdání se takových práv pro případ jiného či následného neplnění či porušení sjednaných smluvních povinností.

14.4. Žádná smluvní strana není odpovědná druhé smluvní straně za vynaložení nákladů, rizika nebo za závazky vyplývající z činnosti této smluvní strany v souvislosti s předmětem plnění. Každá ze smluvních stran bude jednat jako nezávislý právní subjekt, nikoliv jako zmocněnec druhé smluvní strany.

14.5. Smlouvu lze měnit pouze oboustranně odsouhlasenými číslovanými dodatky podepsanými oběma smluvními stranami. Žádný jiný protokol, dokument, obvyklá

praxe nebo zvyk nebudou považovány za dodatek ke Smlouvě nebo za její pozměnění. Výjimkou je postup dle čl. 4.3 této Smlouvy.

14.6. Smluvní strany se dohodly, že žádná z nich není oprávněna postoupit svá práva a povinnosti vyplývající z této smlouvy třetí straně bez předchozího písemného souhlasu druhé smluvní strany, s výjimkou peněžitých pohledávek za druhou smluvní stranou.

14.7. Bude-li některé z ustanovení této smlouvy shledáno jako neplatné nebo nevymahatelné, nemá taková skutečnost vliv na platnost nebo vymahatelnost zbývajících ustanovení této smlouvy.

14.8. Smluvní strany berou na vědomí, že tato smlouva vyžaduje uveřejnění v registru smluv podle zákona č. 340/2015 Sb., v platném znění a s tímto uveřejněním souhlasí. Zaslání smlouvy do registru smluv zajistí kupující neprodleně po podpisu smlouvy. Kupující se zároveň zavazuje informovat prodávajícího o uveřejnění smlouvy v registru smluv tak, že mu zašle kopii potvrzení správce registru smluv o uveřejnění smlouvy bez zbytečného odkladu poté, kdy sám potvrzení obdrží, popř. již v průvodním formuláři vyplní příslušnou kolonku s ID datové schránky prodávajícího (v takovém případě potvrzení od správce registru smluv o provedení registrace smlouvy obdrží obě smluvní strany zároveň).

14.9. Smlouva je uzavírána elektronicky, a to tak, že je opatřena elektronickými podpisy (zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo kvalifikovaným elektronickým podpisem) oprávněných zástupců smluvních stran.

14.10. Nedílnou součástí této smlouvy jsou tyto přílohy:

- Příloha č. 1 – Specifikace a rozsah předmětu plnění
- Příloha č. 2 – Položkový rozpočet
- Příloha č. 3 – Seznam oprávněných osob

14.11. Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Za Security Avengers s.r.o.	Za Univerzitu Karlovu
Ing. Matej Kačic, Ph.D. jednatel	Mgr. Martin Maňásek Kvestor

Příloha 1 – Specifikace a rozsah předmětu plnění

pro veřejnou zakázku

RUK – ÚVT – Sken zranitelností

Zadavatel v rámci projektu Transformace pro VŠ na UK, reg. č. NPO_UK_MSMT-16602/2022 (spolu)financovaného z Národního plánu obnovy bude realizovat pořízení softwarového produktu skenu zranitelností, jeho implementace včetně procesu řízení technických zranitelnosti a poskytnutí související podpory.

Cílem projektu je nasazení bezpečnostní technologie pro skenování technických zranitelností Univerzity Karlovy. Součástí projektu bude také zavedení procesu řízení technických zranitelností.

Rozsah projektu
Skenování technických zranitelností bude primárně zaměřeno na technická aktiva, která zajišťují funkčnost Významných informačních systémů: Studijního informačního systému (SIS), Centrální autentizační služba (CAS), Spisová služba (ESSS), Ubytovací a sociální stipendia a systému IT podpory správy identit uživatelů SIS v rozsahu Systému řízení bezpečnosti informací a dalších informačních systémů a technických aktiv dle potřeb rektorátu a jednotlivých fakult Univerzity Karlovy.

Rozsah projektu bude obsahovat jak nasazení technologie (software) pro skenování technických zranitelností, tak vytvoření, zavedení a optimalizaci procesu řízení technických zranitelností na Univerzitě Karlově. Konkrétně se bude jednat o:

- vytvoření cílového konceptu popisující současný stav a budoucí stav,
- pořízení, nasazení a optimalizace bezpečnostní technologie (SW) pro automatizované skeny zranitelností,
- vytvoření, zavedení a optimalizace procesu řízení technických zranitelností,
- integrace SIEM.

Rozsah skenování počítá se skenováním serverů, infrastrukturních prvků a namátkovým výběrem několika typizovaných koncových stanic, které zajišťují funkčnost Významných informačních systémů na rektorátu Univerzity (RUK).

Běžné i privilegované stanice budou skenovány ad-hoc pomocí samostatných skenerů (bez napojení na centrální správu). Počet samostatných skenerů není omezen a je možné měnit umístění skeneru po uplynutí ochranné doby (10 dnů).

Se zohledněním rozsahu výše uvedeného projektu a plnění smlouvy požaduje Zadavatel následující:

Popis	**Počet**
SW produkt skenu zranitelností pro 500 IP adres včetně podpory a SLA	3
Návrh, nasazení a optimalizaci procesu řízení skenu zranitelností včetně dokumentace	1
Provozní podpora do 30.6.2024	1

1) Požadavky na implementaci díla

Součástí předmětu plnění je:

- Vytvoření harmonogramu implementace (Solution design)
- Dodání programového vybavení (software), specifikovaného v nabídce uchazeče;

- Instalace a konfigurace systému skenu zranitelností
  - Instalace a uvedení do provozu všech komponent,
  - Nastavení kompletní vzájemné komunikace komponent,
  - Aktualizace všech komponent na poslední podporované verze,
  - Nastavení automatických aktualizací,
  - Konfigurace zálohování a archivace
  - Zavedení discovery skenu
    - zavedení skenu zranitelností na prvky pilotního režimu (síťový i privilegovaný sken)
    - zavedení skenu zranitelností na všechny prvky infrastruktury obsažené v tomto projektu (síťový i privilegovaný sken)
  - Návrh časového harmonogramu skenu
  - Nastavení skenů ze samostatných skenerů (nenapojených na centrální správu)
- Kontrola konfigurace přístupů:
  - Kontrola konfigurace rolí/ skupin,
  - Kontrola nastavení oprávnění k monitorovaným zdrojům dle kompetencí,
- Testování a ověření funkčnosti:
  - Otestování funkčnosti skenů zranitelností,
  - Otestování správného generování a obsahu alertů a reportů
  - Otestování oprávnění
- Zpracování dokumentace skutečného provedení v rozsahu:
  - Popis řešení a jeho jednotlivých komponent,
  - Technická specifikace,
  - Provozní dokumentace.
  - Bezpečnostní dokumentace
- Vytvoření, zavedení a optimalizace procesu řízení technických zranitelností,
- Napojení na SIEM zadavatele

2) Správa a provozní podpora díla

Předmětem plnění je taktéž zajištění správy a provozní podpory řešení skenu zranitelností implementovaného v prostředí zadavatele, jeho dalšího rozvoje a to v souladu s článkem 4 smlouvy, která je přílohou č. 3 zadávací dokumentace.
Požadovaná dostupnost je 98% v kalendářním měsíci. Služba zaručené provozní doby 5 dnů x 8 hodin.

<u>Technická specifikace zařízení</u>

Uchazeč vyplní všechny oranžově označené části. Tato příloha slouží k vymezení minimálních technických požadavků zadavatele na poptávané zařízení a ověření jejich splnění. Uchazeč uvede výrobce zařízení, produktové označení nabízeného řešení a parametry nabízeného zařízení prokazující splnění požadované funkcionality/ vlastnosti (případně prohlásí doplněním slova "ANO", že požadovanou funkcionalitu nabízené řešení splňuje, pokud by byl celý popis stejný jako text uvedený v prvním sloupci).

Požadavky na funkcionalitu	**Minimální požadavky**	**Doplní uchazeč dle nabízeného řešení** Způsob naplnění tohoto povinného parametru – tzn. uvedení výrobce, obchodního označení,	**Doplní uchazeč dle nabízeného řešení** Odkaz na přiloženou část nabídky,

		případně uvedení konkrétních parametrů	kde je případně možné ověřit naplnění parametru
Architektura řešení	- On-premise – řešení musí být implementováno v síti Zadavatele a musí být schopno sbírat data a vyhodnocovat zranitelnosti bez nutnosti využití cloudových služeb. - Řešení musí být schopno běžet na virtualizované platformě a na podporovaných operačních systémech RHEL/CentOS, aby se nezvyšovaly licenční náklady na OS. - Možnost distribuovaného nasazení skenovacích agentů do podsítí Zadavatele s napojením na centrální správu. - Možnost skenování ze skenovacích agentů umístěných v externí síti (Internetu).	Všechny požadavky jsou splněny a detailně popsány v kapitole 3.1.	Kapitola 3.1
Architektura řešení	- Řešení musí být schopno běžet na virtualizované platformě a na podporovaných operačních systémech RHEL/CentOS, aby se nezvyšovaly licenční náklady na OS.	Jedná se o on-premise řešení běžící jako virtuální appliance nebo na RHEL/CentOS/Oracle.	Kapitola 3.1
Centrální správa	- Podpora zabezpečeného přístup do management konzole pomocí využití protokolu https ze standardních webových prohlížečů. - Možnost řízení přístupu podle sledovaných systémů (např. administrátoři z jedné pobočky nebudou mít přístup k systémům z druhé pobočky). - Možnost řízení přístupu uživatelů dle předdefinovaných rolí. Možnost nastavení vlastních rolí. - Podpora autentizace vůči Microsoft Active Directory.	Všechny požadavky jsou splněny a detailně popsány v kapitole 3.2.	Kapitola 3.2

	- Automatické aktualizace databáze zranitelností. - Centrální správa musí disponovat přehledovou obrazovkou, kterou si může uživatel přizpůsobit. V rámci přizpůsobení je požadováno alespoň: - možnost zobrazit nejzranitelnější stroje v síti; - zobrazení nejčetnějších zranitelností v síti; - zobrazení počtu zranitelností uvedených v OWASP Top Ten.		
Seznam skenovaných aktiv	- Možnost rychlé identifikace technických aktiv za využití discovery skenování. - Možnost kategorizace aktiv na základě operačního systému, IP adres a dalších atributů. - Možnost dynamické kategorizace aktiv na základě počtu zranitelností, typu zranitelností, přítomnosti konkrétní zranitelností a dalších atributů.	Všechny požadavky jsou splněny a detailně popsány v kapitole 3.3.	Kapitola 3.3

Skenování zranitelností	- Možnost definovat šablony skenů pro jednoduché vytváření více stejných skenů pro různé systémy.
	- Možnost definovat skenovaný systém pomocí statické a dynamické kategorizace aktiv.
	- Skenování za pomoci časového harmonogramu.
	- Možnost autentizovaného skenu:
	  - OS Microsoft Windows;
	  - OS Linux;
	  - pomocí SSH.
	  - Databáze (MSSQL, Postgre, apod.)
	- Řešení musí obsahovat předdefinované šablony pro jednoduché spuštění skenů zranitelností bez nutnosti složité konfigurace.
		Všechny požadavky jsou splněny a detailně popsány v kapitole 3.4.	Kapitola 3.4

	- Možnost definovat vlastní sken bez nutnosti využít předdefinované šablony.		
Kontrola souladu s bezpečnostní politikou	- Řešení musí být schopno zkontrolovat konfiguraci skenovaného systému vůči standardizovaným bezpečnostním politikám (např. CIS). - Řešení musí umožňovat kontrolu konfigurace vůči vlastním bezpečnostním politikám Zadavatele.	Všechny požadavky jsou splněny a detailně popsány v kapitole 3.5.	Kapitola 3.5
Vyhodnocení výsledků	Řešení musí umožňovat analýzu detekovaných zranitelností a poskytovat minimálně následující informace o zranitelnosti: - IP adresa a DNS stroje, na němž byla zranitelnost detekována; - operační systém stroje, na němž byla zranitelnost detekována; - závažnost zranitelnosti; - CVE zranitelnosti; - CVSS skóre; - datum zveřejnění zranitelnosti; - datum první identifikace v síti Zadavatele; - datum poslední identifikace v síti Zadavatele; - datum zveřejnění záplaty (v případě, že byla zveřejněna) - možnost exploitace a náročnost exploitace; - popis zranitelnosti; - návod na odstranění zranitelnosti. - Řešení musí umožnit filtrovat zranitelnosti dle výše uvedených parametrů.	Všechny požadavky jsou splněny a detailně popsány v kapitole 3.6.	Kapitola 3.6

	- Řešení musí poskytovat obrazovku s přehledem: - všech detekovaných zranitelností; - zranitelností detekovaných konkrétním skenováním; - zranitelných strojů specifikovaných IP adresou nebo DNS názvem s počtem zranitelností jednotlivých závažností; - zranitelností seskupených dle portu. - Řešení musí být schopno oddělit zranitelnosti od položek konfigurace, které nejsou ve shodě s bezpečnostní politikou. - Řešení musí umožnit vytvoření výjimky pro konkrétní zranitelnost případně snížení její závažnosti. - Řešení musí disponovat vlastním ticketovacím systémem s možností vytvořit ticket na konkrétní zranitelnost a přiřadit definovanému uživateli.		
Reporting	- Řešení musí poskytovat reporting ve formátu PDF a CSV. - Možnost využít předdefinovaných šablon. - Možnost vytvoření vlastního reportu bez využití šablon. - Řešení musí umožňovat vytvořit vlastní report s možností filtrování zranitelností dle parametrů uvedených v prvním bodě kapitoly „Vyhodnocení výsledků“.	Všechny požadavky jsou splněny a detailně popsány v kapitole 3.7.	Kapitola 3.7

	- Řešení musí umožňovat přidání vlastních komponent do reportu (tabulky, grafy, texty), aby si mohl Zadavatel přizpůsobit reporty svým požadavkům a vytvářet reporty pro různé úrovně managementu. - Možnost automatického reportování po vykonání skenu a odeslání na specifikované emailové adresy. - Možnost pravidelného reportování za pomoci časového harmonogramu.		
Integrace	- Řešení musí být schopno integrace na systémy SIEM. - Řešení musí být schopno integrace na systémy správy privilegovaných účtů za účelem poskytnutí přihlašovacích údajů pro autentizované skeny. - Řešení musí disponovat rozhraním API pro integraci s interními systémy zákazníka.	Všechny požadavky jsou splněny a detailně popsány v kapitole 3.8.	Kapitola 3.8

Nabídka vulnerability management řešení Tenable Security Center

Univerzita Karlova, Rektorát

Security Avengers

Obchodní informace

Obchodní jméno:
Security Avengers s.r.o.

Právní forma:
společnost s ručením omezeným

Rok založení:
2020

Sídlo společnosti:
Kaprova 42/14, Staré Město, 110 00 Praha 1

Statutární zástupce:
Ing. Matej Kačic, jednatel

Kontaktní údaje:
[redacted]

Web:
www.avengers.cz

IČ:
09617477

DIČ:
CZ09617477

Zápis v OR:
C 339054 vedená u Městského soudu v Praze

Bankovní spojení:
[redacted]

Zástupce v tomto jednání:
Matej Kačic
[redacted]

Proč zvolit Security Avengers

Náš tým má bohaté zkušenosti s řešením problémů našich partnerů v oblasti informační bezpečnosti, realizací projektů, technologických dodávek a jejich následné podpory. Navrhoval a implementoval více jak deset projektů perimetrového a interního firewallu datového centra, navrhoval, implementoval, následně spravoval a rozvíjel skenery zranitelností včetně hardeningu mnoha platforem, navrhoval a zabezpečoval koncové stanice, řešení pro monitoring bezpečnostních událostí, pro přístup privilegovaných uživatelů, balancing a aplikační firewally, analyzoval, vytvářel bezpečnostní dokumentace, plány, pomáhal s návrhy architektur a strategií bezpečnosti, auditoval bezpečnostní technologie, pracovní stanice, operační systémy, prováděl penetrační testování, školil a další.

Máme zkušenosti především s finančním sektorem, průmyslem, oblastí zdravotnictví, utility a pojišťovnictvím.

Naši specialisté jsou certifikovaní na celé portfolio produktů Tenable, jako jediní v ČR vlastníme nejvyšší možnou certifikaci úrovně Expert, dále pak na oblast endpoint řešení různých výrobců (např. CrowdStrike, Sentinel One atd.), Next Generation firewall a na celé portfolio Check Point, F5, systémy pro privilegované uživatele BeyondTrust, SIEM a další.

S produkty od společnosti Tenable pracují naši specialisté přes osm let a v této oblasti máme nejzkušenější tým v České republice.

8

let praktických zkušeností s produkty Tenable

60

návrhů, implementací vulnerability management řešení

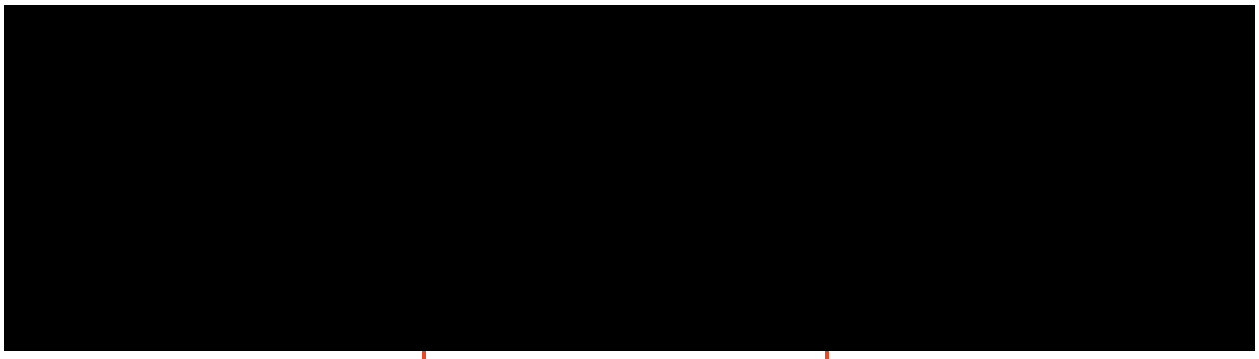
35

hardenovaných platforem

Expert

nejvyšší možná technická certifikace na produkty Tenable (jediná v ČR)

#WeAreAvengers



50+
návrhů síťové bezpečnosti

50+
bezpečnostních auditů

25+
projektů ve finančních institucích

15+
implementací firewallů

150+
bezpečnostních konzultací

15+
let v oboru

20+
návrhů vulnerability a patch management procesu

40+
implementací vulnerability management nástrojů

60+
realizovaných vulnerability assessment projektů

30+
projektů hardeningu OS, databází, webových serverů

35+
bezpečnostních konzultací

8+
let v oboru

10+
návrhů vulnerability a patch management procesu

20+
implementací vulnerability management nástrojů

20+
realizovaných vulnerability assessment projektů

30+
projektů hardeningu OS, databází, webových serverů

10+
bezpečnostních konzultací

4+
let v oboru

Reference týmu


Reference společnosti Security Avengers

Obsah

1 Stručné shrnutí nabídky

Security Avengers předkládají nabídku na vulnerability management Tenable Security Center (dříve Tenable.sc) pro Univerzitu Karlovu (dále jen „UK“).

Nabídka je předložena na základě veřejné zakázky „RUK – ÚVT – Sken zranitelností“. Na základě technické specifikace jsme se rozhodli nabídnout vám řešení od společnosti Tenable – on-premise Tenable Security Center.

Tenable Security Center je on-premise produkt pro řízení zranitelností s pokročilými funkcemi reportingu, analýzy, prioritizace a možnostmi vlastních integrací pomocí REST API. Poskytuje možnost skenování zranitelností a konfiguračních nedostatků. Jedná se o jeden z nejlepších produktů na trhu z hlediska pokrytí databáze zranitelností, přesnosti skenování, míry false positive a možnosti kontrolovat konfiguraci množství různorodých platforem cílových zařízení vůči například CIS benchmarkům.

Tenable Security Center je nabízeno jako subscription ve variantě provozované na 3 roky pro 500 IP adres.

Mezi hlavní přínosy našeho řešení patří zejména:

- Nejlepší řešení na trhu z hlediska pokrytí databáze zranitelností a rychlosti reakce na nově zveřejněné zranitelnosti[1].
- Prioritizace zranitelností pomocí VPR hodnocení postaveném na více než 180 různých parametrech.
- Zohlednění aktuálního zneužívání dané zranitelnosti ve světe při prioritizaci.
- Rozsáhlé možnosti customizace reportů a dashboardů.
- Dynamická kategorizace aktiv na základě typu zařízení, OS, instalovaného softwaru a další.
- Možnost využití agent-less i agent-based skenů, stejně jako skenování z cloudových skenerů.
- Rozhraní REST API pro účely integrací a automatizace.

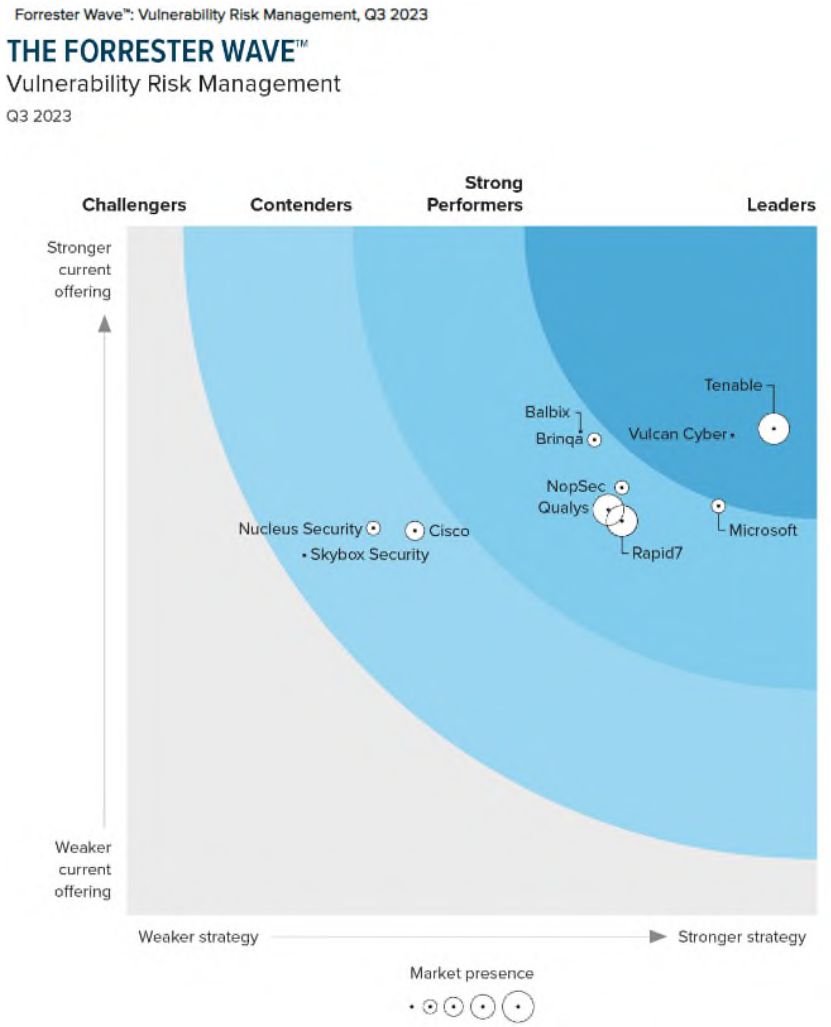
Co může nabídnout tým Security Avengers:

- S produkty od společnosti Tenable pracujeme na denní bázi jak z pohledu implementátora, tak z pohledu zajištění jeho provozu a outsourcingu.
- Náš tým má zkušenosti se zakázkami podobného typu.
- Navrhoval a implementoval více jak třicet projektů skenování zranitelností a hardeningu.
- Dostali jsme reference od velkých zákazníků.
- Naši specialisté jsou certifikovaní na celé portfolio Tenable. Máme nejvyšší technickou certifikaci Expert, kterou náš kolega drží jako jediný v ČR.

[1] https://www.tenable.com/research
https://www.tenable.com/press-releases/tenable-is-number-one-in-vulnerability-and-security-configuration-coverage

2 Stručný popis řešení

Tenable Security Center je vulnerability management nástroj, který vám pomůže s kompletním řízením zranitelností od jejich detekce, přes analýzu, prioritizaci, reporting až po finální mitigaci. Společnost Tenable stojící za tímto produktem je světovým lídrem na trhu v této oblasti, byla zařazena mezi lídry v průzkumu The Forrester Wave – Vulnerability Risk Management 2023.



Nabízený nástroj vám poskytuje možnost skenovat zranitelnosti v prostředí vaší sítě pomocí skenů bez využití agentů, ale zároveň i s možností využít agenty na strojích, kde běžné privilegované skeny nejsou vhodné (notebooky, DMZ, doménové řadiče a další). Stejně tak umožňuje využít cloudové skenery za účelem identifikování zranitelností zjistitelných z prostředí internetu.

Pomocí šablon politik můžete velmi jednoduše nastavit pravidelné skeny vaší sítě, případně je možné využít pokročilou úpravu a vytvoření vlastní skenovací politiky. Využitím credentials (Windows, SSH) získáte možnost detekovat i zranitelnosti, které nejsou síťově zjistitelné, ale jsou zneužitelné například z webového prohlížeče, e-mailového klienta nebo za využití malwaru.

Kromě skenů zranitelností poskytuje nástroj možnost kontrolovat konfiguraci vůči předem stanoveným politikám nebo mezinárodně uznávaným best practice (např. CIS benchmarks). Těmto typům skenů se říká compliance skeny a umožňují porovnávat konfiguraci OS, webových serverů, databází, síťových prvků a dalších systémů vůči hardeningové politice.

Velkou výhodou řešení je prioritizace zranitelností pomocí vlastního hodnocení Vulnerability Priority Rating (VPR), v rámci kterého je hodnoceno přes 180 různých parametrů, včetně aktuálních informací z Threat Intelligence o zneužívání dané zranitelnosti ve světě. Díky tomu máte automatizovanou prioritizaci zranitelností a není nutné vynakládat interní kapacity na opravy zranitelností, které v danou chvíli nejsou z hlediska pravděpodobnosti zneužití prioritní.

Finální částí celého procesu řízení zranitelností je reporting. Nástroj umožňuje informace o zranitelnostech předávat na vlastníky aktiv pomocí pravidelných reportů nebo integrací s libovolným service desk / ticketovacím nástrojem formou nativních nebo custom integrací. Další formy reportingu zajišťuje více než stovka out-of-the-box dostupných šablon reportů a dashboardů, které je možné libovolně customizovat případně vytvořit vlastní reporty či dashboardy.

3 Splnění technických požadavků

3.1 Architektura řešení

Existují dvě verze řešení, které mohou být nasazeny on-premise:

- Virtuální appliance: Tato verze řešení je určena k importu do virtualizačního prostředí.
- Instalační balíčky pro RHEL/CentOS/Oracle systémy: Řešení může být nainstalováno na systémy používající operační systémy RHEL/CentOS/Oracle.

https://docs.tenable.com/general-requirements/Content/SCSoftwareRequirements.htm

https://docs.tenable.com/tenable-core/security-center/Content/TenableCore/Introduction_SC.htm

Řešení nepotřebuje pro svou činnost využívat žádné cloudové služby. Nicméně je nutné pravidelně aktualizovat jeho databázi zranitelností. Tuto aktualizaci lze provádět buď přímo připojením k serverům výrobce, nebo offline aktualizacemi produktu.

https://docs.tenable.com/security-center/6_1/Content/AirGappedEnvironments.htm

Řešení umožňuje nasadit distribuované skenery do sítě, aby bylo možné provádět skenování jednotlivých částí sítě. Taktéž je možné použít agenty, které lze instalovat na koncové systémy. Další možností je nasadit skenery do prostředí mimo interní síť, což umožňuje skenování perimetru a serverů, které jsou dostupné z internetu.

https://docs.tenable.com/security-center/6_1/Content/Architecture.htm

3.2 Centrální správa

Centrální správa je dostupná prostřednictvím webové konzole na portu 443 pomocí protokolu HTTPS. Tato webová konzole je kompatibilní s aktuálními verzemi všech rozšířených prohlížečů, včetně Edge, IE, Chrome, Firefox a Safari.

https://docs.tenable.com/security-center/6_1/Content/PortRequirements.htm

https://docs.tenable.com/security-center/6_1/Content/BrowserRequirements.htm

Řešení umožňuje rozdělovat oprávnění uživatelů systému na základě různých kritérií, jako jsou:

- IP adresy skenovaných systémů.
- Operační systém skenovaných systémů.
- Předdefinované nebo vlastní role.

https://docs.tenable.com/security-center/6_1/Content/UserRoles.htm

https://docs.tenable.com/security-center/6_1/Content/Groups.htm

Pro autentizaci je podporováno ověření vůči Microsoft Active Directory (AD).

https://docs.tenable.com/security-center/6_1/Content/LDAPServers.htm

Aktualizace databáze zranitelností může probíhat pravidelně v předem definovaných intervalech.

https://docs.tenable.com/security-center/6_1/Content/EditPluginsFeeds.htm

Centrální správa nabízí přehledné a plně nastavitelné dashboardy, které mohou zobrazovat různé informace, jako například:

- Nejzranitelnější systémy v síti.
- Zranitelnosti s nejvyšším počtem.
- Zranitelnosti a jejich počet v souladu s OWASP Top Ten.

https://docs.tenable.com/security-center/6_1/Content/Dashboards.htm

3.3 Seznam skenovaných aktiv

Toto řešení obsahuje šablonu pro Host Discovery sken, která umožňuje rychle identifikovat zařízení v síti. Dále obsahuje další šablony pro jednoduché vytváření skenů zranitelností, konfiguračních skenů a dalších.

https://docs.tenable.com/security-center/6_1/Content/ScanningOverview.htm

Detekované systémy lze rozdělit do dvou typů skupin: statických a dynamických.

- Statické skupiny obsahují seznamy DNS nebo IP adres, které jsou předem definované.
- Dynamické skupiny mohou být definovány na základě různých parametrů, včetně:
    - Operačního systému.
    - Nainstalovaných aplikací.
    - Typu zařízení (server, workstation, databáze...).
    - Počtu zranitelností, typu zranitelností a severity zranitelností.
    - Přítomnosti konkrétní zranitelnosti.

https://docs.tenable.com/security-center/6_1/Content/Assets.htm

3.4 Skenování zranitelností

Skeny zranitelností mohou být vytvářeny na základě předdefinovaných šablon, nebo je možné vytvořit vlastní šablony (politiky) podle specifických požadavků.

Šablony pro skenování

- Host Discovey,
- Basic Network Scan,
- Credentialed Patch Audit,
- Web Application Tests,
- Policy Compliance Auditing,
- Atd.

https://docs.tenable.com/security-center/6_1/Content/ScanPolicyTemplates.htm

Cíl skenování lze definovat pomocí IP adresy, DNS nebo na základě přiřazení ke skupině (buď dynamické nebo statické). Všechny skeny umožňují nastavení časového plánu, což umožňuje plánovat skenování na konkrétní časy a dny.

https://docs.tenable.com/security-center/6_1/Content/AddActiveScan.htm

Toto řešení podporuje autentizované skenování vůči různým typům systémů, včetně:

- Operačních systémů (například Windows, Linux s protokolem SSH, macOS s protokolem SSH).
- Databázím.
- Síťovým prvkům (například CISCO).
- Dalším typům systémů, které vyžadují autentizaci při skenování zranitelností.

Využívají se primárně čtyři typy autentizačních údajů:

- Windows – doménový nebo lokální administrátorský účet. Autentizační metody zahrnují použití hesla, autentizačního server Kerberos, LM nebo NTLM hashe a CyberArk Vault.
- SSH – přihlašovací údaje SSH jsou použity pro skenování linuxových systémů, Cisco IOS systémů nebo Unixových systémů. Existuje pět autentizačních metod: pomocí hesla, veřejného klíče, certifikátů, autentizačního serveru Kerberos nebo CyberArk Vault.
- SNMP – použití SNMP community string pro autentizaci.
- Database – přihlašovací údaje pro databázové aplikace Microsoft SQL, Informix/DRDA, DB2, MySQL, Oracle, PostgreSQL.

https://docs.tenable.com/security-center/6_1/Content/Credentials.htm

3.5 Kontrola souladu s bezpečnostní politikou

Kromě skenování zranitelností řešení umožňuje kontrolu konfigurace vůči daným bezpečnostním hardeningovým politikým (tzv. compliance checks). Řešení má out-of-the-box více než 400 auditních šablon pro různé platformy založené na doporučeních CIS benchmarks, DISA a další. Kromě těchto šablon lze vytvořit i vlastní custom auditní soubory pro kontrolu konfigurace vůči vlastním interním hardeningovým politikám.

https://docs.tenable.com/security-center/6_1/Content/AuditFiles.htm

3.6 Vyhodnocení výsledků

Řešení umožňuje provádět podrobnou analýzu zranitelností s poskytnutím informací, jako jsou:

- IP a DNS adresy skenovaného stroje.
- Operační systém a nainstalované aplikace.
- Závažnost zranitelnosti dle hodnocení Tenable, CVSS a VPR (prioritizační metrika Tenable).
- CVE označení zranitelnosti.
- Datum zveřejnění zranitelnosti.
- Datum první identifikace v síti a datum poslední detekce.
- Dostupnost opravy a datum jejího zveřejnění.
- Možnost a náročnost exploitace zranitelnosti.
- Popis zranitelnosti.
- Návod na odstranění zranitelnosti.
- Informace z partnerských služeb Threat Intelligence.

Řešení umožňuje filtrovat nalezené zranitelnosti na základě výše uvedených parametrů. Všechny tyto parametry lze zobrazit v přehledových obrazovkách (dashboardech).

https://docs.tenable.com/security-center/6_1/Content/ViewVulnerabilityInstanceDetails.htm

https://docs.tenable.com/security-center/6_1/Content/ViewHostDetails.htm

https://docs.tenable.com/security-center/6_1/Content/ViewPluginDetails.htm

Řešení poskytuje přehledovou obrazovku obsahující:

- Všechny detekované zranitelnosti.
- Zranitelnosti detekované konkrétním skenem.

- Seznam zranitelných systémů specifikovaných podle IP adresy nebo DNS s počtem zranitelností dle závažnosti.
- Zranitelnosti seskupené dle portu.

https://docs.tenable.com/security-center/6_1/Content/CustomDashboardComponentOptions.htm

https://docs.tenable.com/security-center/6_1/Content/DashboardTemplates.htm

Řešení odděluje detekované zranitelnosti od položek nesouladu (compliance) pro zachování čistých výsledků skenů zranitelností.

https://docs.tenable.com/security-center/6_1/Content/VulnerabilityAnalysisFilters.htm --- filtr Plugin Type

V rámci analýzy zranitelnosti je možné udělit výjimku (akceptovat zranitelnost) nebo manuálně snížit závažnost dané zranitelnosti. Výjimky lze vytvářet hromadně na více než jednu zranitelnost nebo na celé IP adresy. Řešení poskytuje vlastní ticketovací systém, což usnadňuje zavedení procesu řízení zranitelností. Lze vytvořit ticket na konkrétní zranitelnost nebo na seznam zranitelností a přiřadit jej konkrétnímu uživateli k řešení. Vhodnější variantou je ale provést integraci na již provozovaný ticketovací systém.

https://docs.tenable.com/security-center/6_1/Content/AcceptRiskRules.htm

https://docs.tenable.com/security-center/6_1/Content/RecastRiskRules.htm

https://docs.tenable.com/security-center/6_1/Content/Tickets.htm

3.7 Reporting

Řešení poskytuje reporting ve formě desítek předpřipravených šablon, které lze snadno upravovat. Uživatelé systému mohou také vytvářet vlastní reporty bez použití šablon a mají možnost filtrovat výsledky podle parametrů uvedených v části "Vyhodnocení výsledků."

https://docs.tenable.com/security-center/6_1/Content/Reports/ReportTemplates.htm

https://docs.tenable.com/security-center/6_1/Content/Reports/ReportOptions.htm

Řešení umožňuje přidávat vlastní komponenty do reportu, jako jsou:

- Tabulky.
- Grafy (koláčové, sloupcové, spojnicové).
- Textová pole.
- Matice.

https://docs.tenable.com/security-center/6_1/Content/Reports/AddOrEditReportElement.htm

Reporty lze naplánovat na pravidelné spouštění v předem definovaných časech. Dále je možné naplánovat automatické vytváření reportů po dokončení skenování. Řešení umožňuje nastavit automatické odesílání reportů na e-mailové adresy uživatelů.

https://docs.tenable.com/security-center/6_1/Content/Reports/ReportOptions.htm

3.8 Integrace

Řešení je kromě jiného možné integrovat na systémy SIEM a PAM (systémy správy privilegovaných účtů). Kompletní seznam nativních integrací je uvedený níže na odkazu. https://docs.tenable.com/Integrations.htm

Pokud není možné využít nativní integraci nebo pro daný produkt neexistuje, je možné využít REST API pro custom integrace. Stejné API rozhraní lze použít i pro automatizační tasky.

https://docs.tenable.com/security-center/api/index.htm

4 Rozsah implementace

4.1 Příprava pro nasazení

- Vytvoření dokumentu Solution Design, který bude popisovat celou implementaci, síťovou architekturu, HW a SW požadavky, časový harmonogram a další.
- Návrh síťové architektury.
- Dodání SW a licencí.

4.2 Nasazení produktu

- Instalace Tenable Security Center a příslušných skenerů, konfigurace komponent.
- Vytvoření základních skenovacích politik a jejich odladění a otestování.
- Integrace na LDAP a SMTP, vytvoření uživatelů, skupin a rolí.
- Příprava reportů a dashboardů.
- Zavedení discovery skenu:
    - zavedení skenu zranitelností na prvky pilotního režimu (síťový i privilegovaný sken),
    - zavedení skenu zranitelností na všechny prvky infrastruktury obsažené v tomto projektu (síťový i privilegovaný sken).
- Návrh časového harmonogramu skenu
- Napojení na SIEM zadavatele

4.3 Hardening produktu

- Zabezpečení všech komponent systému, nastavení lokálních firewallů.
- Nastavení bezpečnostních funkcí dle best practice.
- Nastavení SNMP monitoringu.
- Automatické aktualizace komponent.
- Nastavení zálohování.

4.4 Přesunutí do produkce

- Příprava a otestování pilotních skenů, případné vyladění politik.
- Nastavení skenování produkčního prostředí.
- Kontrola konfigurace přístupů:
    - Kontrola konfigurace rolí/ skupin,
    - Kontrola nastavení oprávnění k monitorovaným zdrojům dle kompetencí.
- Testování a ověření funkčnosti:
    - Otestování funkčnosti skenů zranitelností
    - Otestování správného generování a obsahu alertů a reportů
    - Otestování oprávnění

4.5 Dokumentace

- Zpracování dokumentace skutečného provedení v rozsahu:
    - Popis řešení a jeho jednotlivých komponent,
    - Technická specifikace,
    - Provozní dokumentace,
    - Bezpečnostní dokumentace.
- Vytvoření, zavedení a optimalizace procesu řízení technických zranitelností.
- Školení pro administrátory systému.

5 Poskytování provozní podpory

5.1 Rozsah podpory

K řešení nabízíme službu technického support zahrnující:

a) profylaktické činnosti, kontrola služeb (1x měsíčně),
b) kontrola provozních logů zařízení (1x měsíčně),
c) návrh případných opatření s cílem předejít možným výpadkům a omezením poskytovaných služeb řešením VMS (dle potřeby, min. 1x měsíčně),
d) odborná technická podpora a odstraňování závad v předmětné oblasti (průběžně),
e) kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce (denně),
f) údržba služby VMS,
g) analýza vhodnosti a potřebnosti implementace opravného balíku (pravidelně při vydání opravného balíku),
h) návrh opatření a postupu implementace opravného balíku ke schválení kupujícímu (pravidelně při vydání opravného balíku).

Ačkoliv je tak uvedeno ve vzoru smlouvy a technické specifikaci, nejsme schopni zajistit „dostupnosti služby VMS (98% za kalendářní měsíc)“, protože nejsme provozovatelem HW vybavení a neručíme za chyby způsobené provozováním produktu, ani za chyby v produktu jako takovém. V rámci poskytování technické podpory však budeme takový incident řešit s nejvyšší prioritou.

5.2 Provozní doba

V pracovní dny od 8:00 do 16:30. Helpdesková aplikace je k dispozici nepřetržitě 24×7.

5.3 Priority incidentů

Na základě závažnosti dopadu Incidentu jsou tyto rozděleny do čtyř (4) priorit:

Priorita 1 – Incident kritické priority

Kritickým Incidentem rozumíme Incident, který může způsobit celkovou nedostupnost Systému, celkovou nefunkčnost systémů v prostředí Objednatele, která má významný dopad na jeho business aktivity.

Priorita 2 – Incident závažné priority

Závažným Incidentem rozumíme Incident vedoucí k nedostupnosti některé z komponent Systému, která ovlivňuje klíčovou funkcionalitu, případně závažně ovlivní funkci/použitelnost dalších aplikací a má dopad na business aktivity Objednatele.

Priorita 3 – Incident běžné priority

Běžným Incidentem rozumíme Incident způsobující nefunkčnost některé z komponent, která nemá přímý dopad na klíčovou funkcionalitu a nemá dopad na business aktivity Objednatele – může se jednat např. o závažnější konfigurační chyby atd.

Priorita 4 – Incident minoritní priority

Minoritním Incidentem je Incident způsoben chybami v konfiguraci, které významně neovlivňují provoz Systému a/nebo nefunkčnost komponent minoritního charakteru, která nemá vliv na business aktivity Objednatele.

5.4 SLA

5.4.1 Měření SLA

SLA: Doba odezvy (IRT) – Je definovaná jako časový interval měřený od doby, kdy Objednatel zadal ticket do Helpdeskové aplikce Poskytovatele (nebo byl automaticky vytvořen Požadavek v Helpdeskové aplikaci Poskytovatele na základě vzájemné integrace helpdeskových aplikací Objednatele a Poskytovatele) do doby, kdy je ticket přijat do řešení Poskytovatelem v rámci jeho Helpdeskové aplikace. Doba odezvy může být také označována jako reakční doba. Vyhodnocení se provádí zvlášť u každého Požadavku Objednatele a je součástí pravidelného měsíčního reportu.

SLA: Doba vyřešení (TRT) – Je definovaná jako časový interval měřený od doby, kdy Poskytovatel přijal (změna stavu ticketu z „New“ na „Open“) ticket do řešení v rámci Helpdeskové aplikace do doby, kdy Poskytovatel vyřešil předmět zadaného ticketu – tedy ticket předal Objednateli ve stavu Resolved a u Bezpečnostních incidentů také vyřešením souvisejícího incidentu v management konzole SentinelOne Objednatele. Měření SLA pro TRT neběží v době, kdy je ticket předán zpět na Objednatele k doplnění informací podstatných k vyřešení ticketu (stav ticketu „Waiting for customer“) a také v době, kdy je ticket předán na podporu výrobce (stav ticketu „Waiting for 3rd party“). V druhém případě začínají běžet SLA, které případně existují mezi Objednatel a výrobcem. Vyhodnocení se provádí zvlášť u každého Požadavku Objednatele a je součástí pravidelného měsíčního reportu.

Omezení pro počítání dob SLA

- Časomíra (tzn. měření skutečných hodnot pro všechny sledované parametry SLA) běží pouze v Době poskytování služby.
- V případě, že Objednatel nesouhlasí s Workaroundem nebo takovéto řešení není funkční, pokračuje časomíra v běhu opět okamžikem vrácení Požadavku k dořešení Poskytovateli.
- Po dobu řešení Požadavku nebo jeho části, které musí provádět třetí strana, je měření doby pozastaveno. Třetí stranou pro účel tohoto odstavce není subdodavatel Poskytovatele.

5.4.2 SLA

Priorita	Doba odezvy (IRT)	Doba vyřešení (TRT)	Způsob řešení	Způsob hlášení incidentů
Kritická	Do 12 hodin	Best effort	Onsite nebo na dálku	Helpdesková aplikace Poskytovatele / e-mail + telefon
Závažná	Do 16 hodin	Best effort	Onsite nebo na dálku	Helpdesková aplikace Poskytovatele / e-mail
Běžná	Do 48 hodin	Best effort	Na dálku	Helpdesková aplikace Poskytovatele / e-mail
Minoritní	Do 48 hodin	Best effort	Na dálku	Helpdesková aplikace Poskytovatele / e-mail
Změnové požadavky / Dotazy	Do 48 hodin	Best effort	Na dálku	Helpdesková aplikace Poskytovatele / e-mail

6 Časový harmonogram projektu

Projekt je členěn do několika fází. Časová náročnost je definována na základě empirických zkušeností s jejich realizací.

Délka projektu představuje čas potřebný k realizaci díla od doby objednání, případně podpisu smlouvy do předání finální podoby zprávy. Fáze projektu na sebe navazují, přičemž některé činnosti se mohou částečně překrývat. Detailní časový harmonogram bude vzájemně odsouhlasen před zahájením projektu. Harmonogram je sepsán bez znalosti prostředí, přičemž minimální délka projektu počítá s hladkým průběhem a maximální reflektuje případné překážky a komunikačním problémy, jež narušují plynulost přípravy díla.

Oblast	Délka projektu
Příprava pro nasazení	2 týdny
Nasazení produktu	2–3 týdny
Hardening produktu	1 týden
Přesunutí do produkce	2–3 týdny
Dokumentace	2 týdny
Celkem	2–3 měsíce

Nutná součinnost

- VPN přístup do prostředí.
- Zajištění síťových prostupů.
- Příprava virtuálních strojů a distribuce OVA virtuálních appliance.
- Testovací virtuální stroj Linux a Windows, testovací privilegované účty.
- Součinnost při nasazení.

Závěr

Všichni Security Avengers pracovali na nabídce s maximální snahou splnit veškeré požadavky Univerzity Karlovy. Věříme, že Vás naše nabídka a návrh v ní obsažený zaujme a budeme pro Vás i jako Avengers nadále kvalitními partnery.

Děkujeme Vám za čas, který jste věnovali prostudování naší nabídky. V případě doplňujících dotazů se na nás můžete kdykoliv obrátit. Doufáme, že naše nabídka splní Vaše očekávání a bude tak moci rozvíjet naše partnerství na poli informační bezpečnosti.

Za společnost Security Avengers s.r.o.

Matej Kačic

#weareAvengers

Příloha č. 2 – Položkový rozpočet

Obsah dílčích nabídkových cen		*Nabídkové ceny*				
		počet	**počet měsíců***	**jednotková cena Kč bez DPH**	**celková cena Kč bez DPH**	**celková cena Kč s DPH**
Software	Softwarový produkt skenu zranitelností 500 IP adres	3	-	525 900,00	1 577 700,00	1 909 017,00
Implementace	Implementace a optimalizace softwarového řešení. návrh, nasazení a optimalizace procesu řízení skenu zranitelností včetně dokumentace.	1	-	160 000,00	160 000,00	193 600,00
Podpora	Provozní podpora	1	9	160 000,00	160 000,00	193 600,00
Celková nabídková cena					**1 897 700,00**	**2 296 217,00**

Příloha č. 3 – Seznam oprávněných osob

Oprávněná osoba	Kupující	Prodávající
Osoba oprávněná jednat ve věcech smluvních	Mgr. Martin Maňásek [redacted]	Ing. Matej Kačic, Ph.D [redacted]
Osoba oprávněná jednat ve věcech technických	[redacted]	
Kontaktní osoby		