Příloha č. 1 Výzvy/Smlouvy - Specifikace předmětu plnění a rozpis celkové ceny na ceny jednotlivých položek

Popis položky	Ks	Cena za jednotku/rok bez DPH (Kč)	Cena za jednotku/rok včetně DPH (Kč)	Celkem za 3 roky bez DPH (Kč)	Celkem za 3 roky včetně DPH (Kč)
Rapid7 – Nexpose – subscription licence na 3 roky	1 000	598 500 Kč	724 185,00 Kč	1 795 500,00 Kč	2 172 555,00 Kč
Metasploit Pro – subscription licence na 3 roky	1	368 500 Kč	445 885,00 Kč	1 105 500,00 Kč	1 337 655,00 Kč
Zaškolení uživatelů a odborná podpora	15MD	Zdarma	Zdarma	Zdarma	Zdarma
Celkem		**967 000 Kč**	**1 170 070,00 Kč**	**2 901 000,00 Kč**	**3 510 210,00 Kč**

* Do tabulky výše doplní uchazeč zadávacího řízení konkrétní nabídkové ceny.

Popis požadavku	povinné parametry	
Vulnerability management systém	**1000 asset**	
Obecné požadavky		
Řešení musí být realizované produkty s integrovaným uživatelským rozhraním včetně dostupnosti výsledků testování, systémově a administrativně snadno ovladatelným aplikačním prostředím.	**ANO**	
Řešení musí být možno provozovat centrální správu a databázi pro důvěrná data on-premise, cloudové rozšíření jsou volitelná, vlastní funkcionalita sběru a vyhodnocení zranitelností musí probíhat čistě v rámci on-premise architektury.	**ANO**	
Zcela bezagentní řešení, tj. bez nutnosti instalace SW kódu na infrastrukturu ICT.	**ANO**	
řešení podporuje i agent based skenování, zejména pro počítače mimo LAN	**ANO**	
Řešení musí umožňovat periodické automatické aktualizace databáze zranitelností a testovací aplikace (scanning engine) na všech skenovacích zařízení (interních i externích v internetu) garantovaná dodavatelem s 24hod reakcí na nově popsané zranitelnosti například na stránkách výrobců SW, nebo online databází zranitelností - cve.mitre.org apod.	**ANO**	
Řešení musí být integrovatelné se systémem McAfee ePO (zdroj assetů, doplňující info o asetech, deployment agentů, poskytování infa do ePO o Risk skore jednotlivých assetů pro navázání politik a automatizovaných akcí), McAfee DXL a TIE (na assetu kde byl přes McAfee TIE reportován Malware zajistí Vuln Manager přirazení Tagu s vyšší rizikovostí) ; Logrhythm SIEM (výstupy skenů zranitelností per asset, compliance a konfiguracni policy) a vmWare (dynamické discovery assetů v rámci virtuálního prostředí, součást security service NSX, pro přímý vulnerability assessments přes hypervisor, asset management, tagování VM strojů na základě úrovně zranitelnosti apod).	**ANO**	
Řešení musí umožňovat přenášení dat mezi jednotlivými komponenty řešení, především mezi centrálním managementem a skenery např. o zjištěných zranitelnostech a informace o testovaných zařízeních, pouze s použitím silného šifrování a pouze v rámci LAN zadavatele (včetně poboček).	**ANO**	

Požadavky na vlastnosti skenování		
Řešení musí umožňovat detekci zranitelností na vzdáleném ICT zařízení s podporou minimálně následujících operačních systémů: Windows desktop 7+ a Windows Server 2008+, RHEL, GNU/Linux distribuce; databází: Oracle, MS SQL Server, PostgreSQL; routerů a switchů s podporou pro IOS, NX-OS, Comware 5 a 7 výrobců HP, Cisco; aplikačních web serverů: Apache, WebSphere, MS IIS; a virtualizační platformy VMware. Dále pak pro Simple Network Management Protocol (SNMP), Secure Shell (SSH), Secure Shell (SSH) Public Key, Telnet, Web Site Form Authentication, Web Site HTTP Authentication, Web Site Session Authentication.	**ANO**	
Řešení musí umožňovat pravidelné automatické, kontinuální (nepřetržité) i ad-hoc ruční spouštění testování zranitelností ICT zařízení v prostředí síťové infrastruktury, s možností výběru IP rozsahu nebo předdefinovaných skupin zařízení a s výběrem/úpravou profilu a zátěže testování - minimální požadovaná periodicita 1x denně přes celý IP rozsah v rámci dodávky. Řešení musí umožnit vizualizaci těchto rozvrhů v kalendáři v rámci GUI.	**ANO**	
Řešení musí umožňovat autentizované skenovaní pro přesnější zjištění bežících služeb a automatizované inteligentní ověřování skutečných síťových služeb běžících na nalezených TCP/UDP portech (nikoliv pouze dle banneru a čísla portu).	**ANO**	
Řešení musí umožňovat volbu intenzity testování (např. kolik IP adres a TCP/UDP portů testovat paralelně), rychlosti testování (např. port mapping speed, packet delay time) s minimalizací zátěže testovaných zařízení a síťové infrastruktury.	**ANO**	
Řešení musí umožňovat nastavení minimalizace rizika výpadku testovaného zařízení nebo síťové služby, minimálně zákazem provádění invazivních testů, zákazem aplikace exploitů, DoS i DDoS útoků a password brute forcingu.	**ANO**	
Řešení musí umožňovat automatické predikce nových zranitelností dle relevantních atributů: verze OS, verze síťových protokolů a verze aplikací na dříve testovaných systémech bez potřeby jejich nového otestování po zveřejnění nových typů zranitelností.	**ANO**	
Řešení musí umožňovat v ceně licence automatizované testování zranitelností webových aplikací s podporou minimálně následujících technik a typů zranitelností: XSS, SQL injection, a další ze seznamu aktuální verze OWASP TOP-10	**ANO**	
Řešení musí umožňovat provádět automatizované testy zranitelností zařízení, systémů i aplikací anonymně (bez přihlášení uživatele) a autentizovaně (pod účtem vybraného uživatele aplikace).	**ANO**	
Řešení musí umožňovat testování dynamicky přidělovaných IP adres přes DHCP službu a sledování její historie a reportování pomocí „DNS name“ nebo „Host name“.	**ANO**	
Řešení musí umožňovat testování překrývajících se IP adres a jejich individuálního sledování a reportování dle různých lokalit.	**ANO**	
Řešení musí paraleně pracovat s IPv4 i IPv6, jedná se především o schopnost detekovat IPv6 systémy při skenování pomocí IPv4.	**ANO**	
Řešení musí detekovat zranitelnosti v celém „IT stacku“. Například po objevení defaultního hesla, toto heslo využít pro další hlubší skeny a detekci souvisejících zranitelností.	**ANO**	

Řešení musí podporovat **automatické zjišťování aktiv (asset management)**, přičemž musí minimálně zvažovat následující parametry IP adresy, MAC adresy a hostname, tak aby bylo zamezeno duplicitám. Systém musí umožňovat načítání logů z DHCP serveru a dynamicky upravovat údaje o strojích, tj. řešení musí umožňovat discovery scan, tedy zrychlené pravidelné automatické, kontinuální (nepřetržité) i ad-hoc ruční spouštění mapování síťové infrastruktury s identifikací i OS, TCP a UDP portů a služeb a vyznačením nových, potvrzených a nepotvrzených zařízení. Minimální požadovaná periodicita 1x denně přes celý IP rozsah v rámci dodávky. Assset manager musí umět čerpat i informace s McAfee ePo a McAfee Rogue senzorů. VM při autentifikovaném skenu dokáže vytvořit i seznam běžících služeb, dle něj se dá pak groupovat, vyhledávat apod (např verze OS, firmware, běžící služby, databáze aj)	**ANO**	
Požadavky na scoring, značkování a filtrace		
Řešení musí umožňovat automatickou aktualizaci tagů v Asset databázi dle těchto dynamických tagovacích pravidel.	**ANO**	
Řešení musí umožňovat automatickou centralizaci všech nalezených aktivních systémů a jejich atributů: verze OS, verze aplikací, otevřené TCP a UDP porty a síťové protokoly do jednotné Asset databáze s možností definovat statické a dynamické hierarchické tagy (nálepky) a dle těchto tagů provádět filtrování aktiv, jejich testování i reportování výsledků.	**ANO**	
Řešení musí podporovat tzv Real Risk skóre, zahrňující do priorizace akcí a kritičnosti zranitelnosti i informace o existenci exploitu a informaci již o použití daného exploitu (nebo jiného zneužití zranitelnosti) včetně zahrnutí informace o obtížnosti zneužití (dokáže i začátečník nebo jen zkušený profesionál apod).	**ANO**	
Řešení musí umožňovat definici pravidel pro automatické a dynamické tagování aktivních systémů dle nalezených atributů po každém testu zranitelností, minimálně pro:	**ANO**	
verzi operačního systému	**ANO**	
verzi instalovaných aplikací	**ANO**	
otevřené TCP a UDP porty	**ANO**	
verzi síťových protokolů	**ANO**	
verzi nalezených zranitelností.	**ANO**	
Řešení musí umožňovat centralizované úpravy v databázi zranitelností, a to tak aby pro celý rozsah implementace bylo možné měnit hodnotu rizikovosti zranitelností, popis hrozeb, popis negativního dopadu a odstranění zranitelností nebo bylo možné vyjmout určité zranitelnosti z testování, a dále editovat CVSS Scoring (Common Vulnerability Scoring System).	**ANO**	
VM pro každou zjištěnou zranitelnost uvádět popis relevantních hrozeb, možného negativního dopadu na systém, odkazy na online zdroje nebo databáze zranitelnosti popisující danou zranitelnost (např. webovou stránku výrobce SW, cve.mitre.org apod.) a popis odstranění zranitelnosti s uvedením http linku na patch výrobce nebo postup změny konfigurace systému.	**ANO**	
Řešení musí umožňovat automatizovanou identifikaci všech zjištěných zranitelností ve výsledcích testování, včetně míry jejich rizikovosti, popisu příslušných TCP/UDP portů, protokolů, síťových služeb a aplikací na kterých byly detekovány.	**ANO**	
Požadavky na vizualizaci		

Řešení musí umožňovat filtrování výsledků mapování síťové infrastruktury dle platformy OS, otevřených TCP-IP portů, potvrzených/nepotvrzených zařízení, automatizované srovnávání historických map s vyznačením rozdílů.	**ANO**	
Řešení musí umožňovat automatické filtrování a reportování relevantních aktiv dotčených novou zranitelností s vyznačením pravděpodobnosti s využitím skóre reálného rizika.	**ANO**	
Požadavky na shodu nastavení		
Configuration control. Řešení musí umožňovat definice a tvorbu i vlastních template bezpečnostní kontroly konfigurací operačních systémů Windows, Linux na základě vybraných parametrů uložených v registrech a souborových systémech a možnost kontrolovat integritu vybraných konfiguračních souborů.	**ANO**	
Řešení musí umožňovat automatické provádění bezpečnostního auditu konfigurace minimálně následujících operačních systémů: Windows desktop 7+ a Windows Server 2008+, RHEL, GNU/Linux distribuce; databází: Oracle 10+, MS SQL Server, Postgres, MySQL; routerů a switchů s podporou pro IOS, NX-OS, Comware 5 a 7 výrobců HP, Cisco; aplikačních web serverů: Apache, WebSphere, MS IIS; a virtualizační platformy VMware; vůči šablonám technických bezpečnostních opatření.	**ANO**	
Požadavky na autentizaci, autorizaci a uživatelskou segregaci		
Řešení musí umožňovat seskupování testovaných systémů do skupin s přiřazením vlastníků a hodnoty aktiv.	**ANO**	
Řešení musí umožňovat katalogizaci rozsahu testovaných webových aplikací pod účtem uživatele a porovnání přístupových práv uvnitř webové aplikace mezi jednotlivými uživateli.	**ANO**	
Řešení musí umožňovat provádět testování zranitelností bez nebo volitelně se vzdálenou autentizací na testovaná zařízení na úroveň operačních systémů a databází.	**ANO**	
Řešení musí podporovat autentizaci uživatelů do centrální řídící aplikace a centrální databáze výsledků testování, pomocí externího LDAP, primárně AD s Kerberos.	**ANO**	
Řešení musí umožňovat centralizované a vysoce zabezpečené šifrované úložiště všech výsledků mapování sítě a testování zranitelností systémů s řízením přístupových oprávnění na základě definovaných rolí a odpovědností k výsledkům a spouštění testování a auditů, dle principu need-to-know.	**ANO**	
Řešení musí podporovat uživatelsky definované zranitelnosti a uživatelskou úpravu stávajících signatur	**ANO**	
Požadavky na reporting		
Řešení musí umožňovat centralizované, agregované ukládání všech výsledků testování zranitelností a auditů konfigurace všech systémů a webových aplikací do jednotné normalizované databáze s centrálním monitoringem stavu zranitelností (formou Dashboardu) a centralizovaným reportingem nad agregovanými výsledky všech realizovaných testů a auditů ze všech lokalit v rámci dodávky.	**ANO**	
Řešení musí umožňovat automatické filtrování a reportování relevantních aktiv dotčených zvolenou „Zero-Day“ zranitelností nebo hrozbou s vyznačením pravděpodobnosti úspěšného útoku.	**ANO**	
Řešení musí umožňovat konfigurovatelný reporting a filtrování výsledků testování, zpracování trendů za libovolné časové období nad historií testování, porovnávání stavu zranitelností za zvolené časové období a oblast sítě a srovnávání výsledků vybraných historických testů.	**ANO**	

Řešení musí umožňovat reporting výsledků mapování a testování zranitelností přes celou infrastrukturu v rámci dodávky, nezávislý reporting nad konkrétními realizovanými testy, reporting s automatickou korelací poslední známé informace a stavu zranitelností nad zvoleným rozsahem reportu.	**ANO**	
Řešení musí umožňovat generování reportu nalezených zranitelností dle optimální logiky instalace patchů od nejnovějších po nejstarší patche a s vyřazením nahrazených patchů novějšími.	**ANO**	
Řešení musí umožňovat podrobný technický reporting všech zjištěných zranitelností, informací a detailů o reportovaných systémech s možností filtrování zvolené úrovně a typu detailu.	**ANO**	
Řešení musí umožňovat vytvořit sumární přehledový manažerský reporting o celkovém stavu a počtu zranitelností, trendem a vyplývající míře rizika nad zvoleným rozsahem reportu.	**ANO**	
Řešení musí umožňovat konfigurovatelný reporting a filtrování výsledků testování webových aplikací s možností třídění a filtrování výsledků testování dle všech kategorií zranitelností aktuální verze OWASP TOP-10 a filtrování výsledků testování dle zvolené topologie (logických větví) webových aplikací.	**ANO**	
Řešení musí umožňovat archivaci výsledků testů min. 12 měsíců s možností exportu minimálně ve formátech XML, CSV, HTM, PDF.	**ANO**	
Řešení musí umožňovat automatickou centrální archivaci a korelaci všech výsledků historických testů zranitelností ze všech testovaných zařízení a oddělení reportingu od jednotlivých výsledků jednotlivých testů.	**ANO**	
Řešení musí konsolidovat zranitelnosti odstranitelné stejným postupem a toto prezentovat formou remediačních plánů v rámci reportů.	**ANO**	
Řešení musí identifikovat zranitelnosti, pro které existuje exploit, případně asociované s konkrétním malware kitem. Řešení musí identifikovat známé typy malware a expoit kity související se zjištěnými zranitelnostmi a tyto skutečnosti zahrnout do rizikovosti zranitelnosti. Součástí popisu zranitelnosti musí být informace, zda je daná zranitelnost využívána útočníky	**ANO**	

Další požadavky	
Hodnocení rizik musí vyjma parametru CVSS zahrnovat typ aktiva, jeho důležitost, dostupnost expoiltů, zneužitelnost dané hrozby útočníkem, technická náročnost zneužití hrozby a další parametry. Výsledkem všech parametrů je ohodnocení dané zranitelnosti z hlediska její kritičnosti.	**ANO**
Řešení musí navrhovat kroky k odstranění hrozby a poskytovat nástroje pro optimalizace počtu kroků opatření s cílem udržet skóre rizikovosti na stanovené úrovni	**ANO**
Řešení musí podporovat integraci se SIEM produkty LogRhythm	**ANO**
Řešení musí podporovat integraci s penetračními testovacími platformami, aby bylo možné potvrdit, že zranitelnosti lze využít, například integraci s Metasploit	**ANO**
Řešení muselo být hodnoceno v rámci Forrester Wave 2018 jako Leader nebo Strong performer	**ANO**
Řešení musí obsahovat mechanizmus pro nastavení minimálních politik pro jednotlivá aktiva a reportovat neshodu s politikami	**ANO**
Řešení by mělo obsahovat automatický mechanizmus k označování strojů (např. dle parametrů) a na základě označení provádět další akce. Systém musí obsahovat také ruční značení strojů	**ANO**
Řešení musí být schopno automaticky kategorizovat prostředky na základě více atributů (například nainstalovaný operační systém, IP rozsah) a stroje objevené při skenování automaticky třídit do dané skupiny	**ANO**

Řešení musí umožňovat také autentizované skenování. A systém musí pro atentizaci podporovat minimálně tyto systémy: Concurrent Versioning System (CVS) DB2; File Transfer Protocol (FTP); IBM AS/400; Lotus Notes/Domino Microsoft SQL Server ; Sybase SQL Server Microsoft Windows/Samba (SMB/CIFS); Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS) MySQL Server; Oracle Post Office Protocol (POP); PostgreSQL Remote Execution; Simple Network Management Protocol (SNMP) Secure Shell (SSH); Secure Shell (SSH) Public Key Sybase SQL Server; Telnet; Web Site Form Authentication	**ANO**