Příloha č. 1

ke Smlouvě o poskytování služeb uzavřené na základě veřejné zakázky s názvem „Služba řízení technických zranitelností IS a služby podpory na 36 měsíců "

Podrobné technické požadavky na řešení

Podrobné technické požadavky na řešení Skeneru technických zranitelností ŘTZ		
	Funkční požadavky nabízeného řešení	**Závaznost**
	1. Vlastnosti systému	
Základní funkce	Automatické testování zranitelností zařízení a aplikací, které jsou součástí síťové a komunikační infrastruktury.	Povinné
	Všechna data a výsledky skenování jsou uloženy v rámci zákazníkovi lokální instance (on premise) v místě provozu HW appliance.	Povinné
	Podrobná definice auditu do úrovně rychlosti komunikace vůči zařízení, použitých modulů a technik, včetně definice časového rozsahu daného testu.	Povinné
	Všechny aktivity lze nastavit pomocí plánování a workflow managementu, kde uživatel může sestavit přesný postup v rámci testu.	Povinné
	Volba intenzity skenování T1-T5, pps (packet per second), typu discovery (ARP ping, ICMP ping, UDP ping, TCP ping, časového rozsahu testu, nahodilosti dotazu v testu, počtu vláken vůči jedné IP, volba použitých modulů, včetně možností prolamování hesel (bruteforce) vůči jednotlivým službám.	Povinné
	Možnost přednastavit přihlašovací údaje pro různé typy služeb HTTP (JWT, basic, NTLM, token, cookies) SSL Cert, SSH, SMB, SNMP, RDP atd.	Povinné
	Definice automatického skenování pomocí workflow.	Povinné
API a integrace	Součástí je dokumentované API pro přístup k datům a k zápisu dat do jednotlivých modulů a součástí řešení:	Povinné
	- Integrace se SIEM: QRadar, FortiSIEM, Fidelis, Log360,	Povinné
	- Integrace s IDS (systémy detekce průniku): Fidelis, Suricata, Snort, Log360,	Povinné
	- Integrace s MS Active Directory, LDAP.	Povinné
	Všechny funkce přístupné přes CLI.	Povinné
	Součástí je dokumentované API pro přístup k datům a zápisu dat do jednotlivých modulů a součástí řešení.	Povinné
Nastavení správy,	Centrální správa uživatelů, senzorů, agentů a jednotlivých instancí.	Povinné

filtrování a auditu	Kompletní zprávu zranitelností, IP, auditu, strojů, aplikací v rámci assets, včetně filtrování a řazení dle jednotlivých atributů.	Povinné
	Filtrace dat dle OWASP top ten, OWASP, vlastních metodik nebo skupin. Definice vlastních tags a assets groups.	Povinné
	Audit lze zadat na základě filtrace assets / assets group.	Povinné
	Možnosti provádění discovery sítí bez vulnerability testů nebo dalších auditů.	Povinné
	Kategorizace zdrojů, IP, systémů, aplikací v rámci assets (správa zdrojů).	Povinné
Konfigurace a možnosti skenování	Možné konfigurace testování:	Povinné
	Definice vlastních šablon nebo kopírování předchozího nastavení testu	Povinné
	Možnost sestavení vlastního testu	Povinné
	Možnost plánovat jednotlivé testy pomocí workflow nebo plánovače úloh	Povinné
	Provádění testu ve shodě s definovaným compliance	Povinné
	Filtrování zranitelností pomocí:	Povinné
	IP adresy nebo jeho sítí, DNS názvu nebo jeho části, NetBIOS názvu nebo jeho části	Povinné
	Operačního systému stroje nebo jeho části, verze OS, kategorie OS	Povinné
	Závažnosti zranitelnosti, včetně definice remote/local a exploitovatelnosti dané zranitelnosti, včetně dostupnosti funkčního exploitu na danou zranitelnost.	Povinné
	CVE zranitelnosti, CWS kategorie zranitelnosti, CVSS skóre verze 2.0, 3.0,	Povinné
	Kompatibilita s Qualys score	Povinné
	Datum zveřejnění nebo aktualizace	Povinné
	Datum první nebo poslední identifikace zranitelnosti v síti	Povinné
	Popis zranitelnosti včetně doporučeného řešení	Povinné
	Kompletní sestavy přehledů:	Povinné
	Všechny detekované zranitelnosti	Povinné
	Všechny zranitelnosti detekované na základě určitého testu	Povinné
	Podle IP, služeb, DNS názvu a NETBIOS názvu	Povinné
	Portů	Povinné
	Definice zranitelnosti podle bezpečností politiky nebo compliance	Povinné
	Možnost redefinice úrovně zranitelnosti, ignorování případně potlačení zranitelnosti.	Povinné

Reportování	**Vytváření reportů**	
	Reporty ve formátu HTML, PDF, XML, CSV, JSON, XLS, reporting systém umožňuje definovat vlastní výstupní formát dat.	Povinné
	Předdefinované šablony, včetně skriptovacího a template jazyka.	Povinné
	Možnost vlastní tvorby reportu, včetně výstupního formátu, součástí je dokumentace.	Povinné
	Možnost v rámci auditu definovat cíle, aplikace, služby a zranitelnosti, které budou zahrnuty v rámci auditu. U zranitelnosti je možné provést rescoring (změna úrovně zranitelnosti) chyb na základě požadavku uživatele.	Povinné
	Plné uživatelské nastavení reportu součástí reportovacího modulu.	Povinné
	Při tvorbě auditu je možné nastavit notifikační e-mail o dokončení testu a zároveň zaslat na požadovaný e-mail hotový report.	Povinné
	Plánování jednotlivých reportů a aktivit pomocí plánovače událostí a definice vlastního workflow pro automatizaci operací.	Povinné
	Komunikace technologií M2M mezi senzory, funkce master mode s funkcí samostatných senzorů.	Povinné
Zabezpečení skeneru a přihlašování	**Zabezpečení nabízeného řešení**	
	Webové rozhraní pro administraci řešení přístupné přes HTTPS, autorizace uživatele s podporou OTP/2FA autorizace.	Povinné
	API přístupné přes HTTPS, s autorizací přes JWT/Baerer token.	Povinné
	Administrace uživatele včetně jejich práv k auditu, reportu, assets a jednotlivým modulům.	Povinné
	Limitace přístupu uživatele k aplikaci na základě IP ACL, limitace uživatele vůči IP, se kterými smí pracovat.	Povinné

HW a SW, licencování a ostatní požadavky	**2. Hardware včetně všech licencí SW pro provoz 36 měsíců**	
	On premise řešení (řešení a data uložena u odběratele služby).	Povinné
	Rozsah licence pro skenování 5000 zařízení/IP adres, licence se aplikuje na všechny aktivity po tzv. Discovery služeb.	Povinné
	Kapacita testování: 5.000 IP za 24 hodin.	Povinné
	HW appliance připravena pro instalaci do 19-palcové skříně. HW pro sondu tvoří 1U, HW pro jádro 2U-4U podle velikosti instance.	Povinné
	Porty: 4x1Gbps LAN/Ethernet Cat5e	Povinné
	Porty: 2xSFP 10Gbe SFP+	Povinné
	Napájení: redundantní zdroj 2x500 W HW Sonda, redundantní zdroj 2x800 W HW jádro.	Povinné

	Součástí jsou teleskopické ližiny pro montáž do 19-palcové skříně, včetně cable managementu.	Povinné
	Instance 5.000 IP umožňuje až 6 senzorů v libovolných lokalitách.	Povinné
	Součástí ceny je zaškolení obsluhy rozsahu 2x 4 hodiny pro 10 osob, lze rozložit na menší bloky.	Povinné
	Odpovědnost za vady, termíny provedení zásahů a reakční doba je součástí SLA - NBD přihlášení do 16 hod.	Povinné
	Revize interní dokumentace k systému ŘTZ v rozsahu 5 čld (člověko-dny).	Povinné
	Podpora pro řešení incidentů 7x24.	Povinné
	Zpravodajství o hrozbách – poskytnou reportů zranitelností povědomí o aktuálním prostředí hrozeb vůči infrastruktuře ICT organizace z interních a externích zdrojů, návrh opatření k jejich zmírnění.	Povinné

Významový slovník:

Zkratka	Popis / význam
OWASP	Open Web Application Security Project
M2M	Machine to Machine – přímá komunikace mezi zařízeními komunikačním kanálem
CVE zranitelnosti	common vulnerabilities and exposures - běžné zranitelnosti a chyby v zabezpečení
CWS kategorie zranitelnosti	Common Weakness Scoring – systém pro prioritizaci SW slabostí v konzistentním, flexibilním a otevřeném formátu
CVSS skóre	Common Vulnerability Scoring System - systém hodnocení závažnosti bezpečnostních zranitelností počítačových systémů
IDS	Intrusion Detection Systems – systém detekce narušení / systém pro detekci průniku
IAS	Identity and Access Services - systém pro správu identit a přístupu k informacím
NAC	Network Access Control – bezpečnostní technologie, spravující přístup k síti a jejímu zabezpečení proti neoprávněnému přístupu
CP	Centrální pracoviště
DC	Datové centrum
KBÚ/KBI	Kybernetická bezpečnostní událost / Kybernetický bezpečnostní incident
IS	Informační systém