# 18 Nástroj pro vulnerability management

V zájmu zajištění schopnosti detekovat potenciální zranitelnosti na externě i interně dostupných prvcích IT infrastruktury požadujeme dodání nástroje (případně souboru nástrojů) pro bezpečnostní testování/testování zranitelností.

S ohledem na vysokou citlivost zpracovávaných dat musí být všechny dodané nástroje schopné instalace všech komponent (včetně managementu) na prvky umístěné v lokální síti, která je pod správou Zadavatele. Výstupy z testů/skenů musí být rovněž zpracovávány lokálně bez jejich zasílání do cloudu. Dodaný nástroj/nástroje musí umožňovat ovládání s pomocí webového GUI.

Dodané řešení musí podporovat realizaci vzdálených bezagentských privilegovaných i neprivilegovaných skenů neomezeného počtu zařízení umístěných v interní síti. Pro zajištění schopnosti realizace externích testů, zařízení mimo doménu a testů zařízení v DMZ musí řešení zároveň poskytovat možnost instalace dodatečných centrálně řízených skenerů mimo interní síť a nasazení agentů na vybrané stroje. Prostřednictvím těchto nástrojů musí podporovat bezpečnostní testování/skenování alespoň 128 zařízení.

Instalaci agentů a skenerů musí být možné realizovat na prvky s operačními systémy Microsoft Windows 7 a vyšší, Microsoft Windows Server 2008 a vyšší, macOS i Linux. Řešení musí být obecně schopné realizovat bezpečnostní testy/skeny koncových zařízení a serverů s operačními systémy Windows, Linux i macOS.

Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech. V rámci výstupů musí být řešení schopné poskytovat informace o CVE spojených s detekovanými zranitelnostmi a o dostupnosti relevantních záplat, nebo jiném způsobu eliminace zranitelností (workaround). Zranitelnosti a další zjištění musí být výsledným řešením automaticky dle závažnosti kategorizovány do alespoň 5 skupin. Pro konkrétní zranitelnosti/zjištění na specifických systémech musí být možné manuálně upravit (snížit/zvýšit) jeho závažnost v závislosti na specifikách konkrétních systémů.

Řešení musí být schopné zobrazovat historický vývoj počtů a závažností zranitelností pro jednotlivé skenované systémy, nebo jejich skupiny, pokud byly všechny skenovány stejným způsobem souběžně. Pro jednotlivé systémy tak bude možné sledovat vývoj počtů zranitelností a jejich úspěšné eliminace.

Pro potřeby reportingu musí řešení poskytovat schopnost exportu výsledků minimálně ve formátech CSV a HTML. Výsledky skenů musí být rovněž možné exportovat ve výše uvedeném nebo jiném formátu umožňujícím provedení jejich opětovného importu do skeneru.

Součástí dodávky bude i převod licencí relevantního nástroje/nástrojů na zadavatele s podporou po dobu 5 let včetně update či upgrade a jeho/jejich implementace do prostředí v době realizace i podpory.

Součástí dodávky bude i HW, licence VMware a OS nutný pro provoz nástroje, který budou zahrnut do technického opatření *„Doplnění HW Datového centra o servery a pole“*.

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| Schopnost provádět vzdálené privilegované skeny | ANO |  |
| Schopnost provádět vzdálené neprivilegované skeny | ANO |  |
| Podpora většího počtu skenerů a distribuovaného skenování | ANO |  |
| Schopnost skenovat vzdáleně neomezené množství koncových IP adres | ANO |  |
| Schopnost připojení minimálně 128 agentů pro realizaci agent-based testů/skenů | 128 |  |
| Podpora skenů webových aplikací | ANO |  |
| Prodloužená technická podpora navrženého řešení | 60 měsíců |  |