Server s grafickým adaptérem 3 ks

Požadované parametry:

Požadované parametry server
standardní rozměry RACK (šíře 19“ a výška 2U) možnost mixovat SATA, SAS a NVMe disky (min. 8 NVME portů na server)
trvalý provoz v prostředí do 35°C
vzdálená správa serverů nezávislá na operačním systému umožňující vzdálené vypnutí, zapnutí, restart, vzdálený přenos konzole, kontrolu HW logů, nastavení bootování z virtuálních disků (IMM), včetně LCD display na přední straně, ze kterého je možné odečíst minimálně IP Adresu management procesoru a vnitřní zdraví serveru.
Zařízení musí být certifikované pro(certifikaci musí být možné ověřit na stránkách výrobce SW):
Windows Server 2022
VMware v aktuální verzi
Server v nabízené konfiguraci musí být kompatibilní s aktuální verzí VMware hypervizoru a virtualizaci desktopů. Všechny komponenty serveru musí být prokazatelně certifikovány VMware HCL a to i pro oblast SDS(software defined storage). Komponenty musí být uvedeny na https://www.vmware.com/resources/compatibility/search.php
CPU v serveru musí:
být 64-bitové, Intel poslední generace
mít minimálně 2x CPU
mít minimálně: - 8 jader - 3,2 GHz - SPEC CPU2017 Floating Point Rate Reseult min. 168 bodů při plném osazení. Test musí být zveřejněný pro konkrétní CPU v konkrétním nabízeném serveru
RAM osazená v serveru musí mít minimálně:
Celkovou kapacitu 768 GB
Min. 3200 Mhz
V případě plného osazení rozšiřitelnost až na 8 TB
RAID řadič osazený v serveru musí mít minimálně:
Diskové HBA, které je centifikované pro VMware vSAN a je uvedeno nna compatibility listu pro VMware VSAN: - Podpora 12Gbit/s SAS - Podpora min 24 ks disků
HDD osazené v serveru musí mít minimálně:
Min. 24 x 2,5“ disků SATA/SAS/NVMe, kdy každý disk musí mít minimálně: - 1 x 800GB SSD 12G SAS, min 10DWPD - 6 x 3,84 TB SSD 12G SAS, min 1 DWPD
rámeček s libovolným diskem musí být možné vyměnit bez nástrojů (hot-plug)
Osazeno 2× disk SSD M.2 240 GB v RAID 1
LAN osazené v serveru musí mít minimálně:
Min. 4 x 10/25 Gbit/s + 2 x 1Gbit/s
Porty serveru minimálně:
Min. 1 x Interní USB 3.0 port
Min. 1x USB port na přední straně pro připojení do management serveru
Min. 2 x PCIe x8 a 4 x PCIe x16
PS v serveru musí být minimálně:
mít minimálně 2x PSU
Výkon min. 1300W AC
být vzájemně redundantní

se stejným výkonem
vyměnitelné bez nástrojů
podporovat standardní „euro“ konektor
Grafická karta osazená v serveru musí být minimálně těchto parametrů:
Musí být kryta stejným HW a SW supportem jako server
Paměť min. 4 x 16GB, s propustností min. 4 x 200 GB/s
Min. 4x 1280 Cuda jader
Interface min. PCIe Gen4
Chlazení passivní, s velikostí Full height, full length (FHFL) Dual Slot
Podpora akcelerace VDI
Licence pro akceleraci virtuálních PC s podporou na 5 let min. 27 ks
Z důvodu kompatibility vyžaduje zadavatel Serverovou kartu NVIDIA
Managment:
Licence pro doživotní vzdálený management, včetně plné remote presence a mapování vzdálených medií, kompatibilní s již provozovaným management iDrac 9.
Management serveru umožňuje vzdáleně mapovat media ISO, CD nebo DVD, Floppy a USB Disk.
Dedikovaný management Ethernet a USB port pro management serveru
Webové rozhraní HTML5 pro management serveru
Přístup na OOB management pomocí protokolů IPMI 2.0, DCMI 1.5, CLI, SSH, Telnet, SMASH-CLP, WSMAN, Redfish, COM port
Možnost uzamčení systému proti instalaci upgradů
Správa napájení včetně omezení příkonu
Automatická aktualizace FW
Možnost spravovat více serverů z jednoho místa bez nutnosti instalace dalšího software
Možnost bezpečného resetování všech komponent serveru a uvedení do počáteční konfigurace, včetně vymazání dat na discích.
Server musí umožňovat „lock-out“ BIOSu a firmware jednotlivých komponent tak aby bylo zabráněno přepisu závadnou aktualizací.
Možnost nastavení parametrů a odečet stavu serverů a logů pomocí mobilního telefonu (Android, iOS), bez nutnosti kabelového připojení.
Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)
Webové rozhraní výrobce musí umožňovat: - připojení do centrálního dohledu výrobce, - ověřování stavu záruky dle sériového čísla serveru - stahování ovladačů a manuálů, aktualizací firmware včetně bezpečnostních záplat pro konkrétní zadané produktové nebo sériové číslo zařízení
Aktualizace firmware jednotlivých subkomponent pomocí automatického prostředku výrobce serveru, nikoliv ručním pouštěním jednotlivých binárních souborů Tyto prostředky podpory musí být dostupné
Součástí nabízeného řešení musí být minimálně tyto dva nástroje: · Nástroj pro automatizovanou a trvale aktualizovanou kontrolu aktuální kompatibility klíčových komponent řešení (HW, SDS, virtualizační platforma) vůči průběžně aktualizované online certifikační matici výrobce řešení. · Nástroj pro instalaci nových verzí firmwaru/sw komponent – v automatizovaném režimu. Instalace je prováděna jako automatizovaný proces se zachováním logické souslednosti jednotlivých kroků procesu. Použití obou nástrojů musí být bezvýpadkové – po dobu údržby clusteru je nutné mít zachovanou funkčnost provozovaných aplikací.

Zadavatel požaduje, aby bylo možné připojit do zadavatelem požadovaného management a monitoring nástroje . Tato platforma slouží jako konsolidovaný monitoring pro různé komponenty DC. Nástroj musí být umístěný v Cloud prostředí s přístupem anytime, from anywhere včetně přístupu z mobilní aplikace, včetně push notifikací. Součástí dodávky serverů musí být monitorovací SW 1:many, bez licenčního omezení počtu monitorovaných zařízení, s přístupem kdykoliv, odkudkoliv bez nutnosti připojování se VPN do vnitřní infrastruktury zadavatele. Monitorovací systém musí mít k dispozici zdarma mobilní aplikaci s podporou push notifikací pro Android a Apple iOS).
Možnost integrace management serveru do již provozovaného nástroje: Dell Open manage. Integrace do úrovně aplikace FW a konfiguračních změn managementu spravovaného server.
Další služby:
Záruka výrobce na 5 let na HW i SW (včetně update), s registrací na jméno Kupujícího a ověřitelnou na webu výrobce, s reakční dobou na servisní zásah 8x5 Next-Business-Day (reakční doba do následujícího pracovního dne od nahlášení, s hlášením možným 8 hodin denně/5 dnů v týdnu), s opravou/výměnnou v místě, servisním technikem (on-site). Možnost zadávat servisní požadavky 24 x7. Možnost zadávat servisní požadavky na webu, telefonicky nebo emailem. Všechny tyto způsoby musí být zveřejněny na webu výrobce server s konkrétním telefoním číslem, nebo emailem. Zařízení jako celek musí být určeno pro český trh a kryto identickým SLA a délkou záruky jako je požadováno v této ZD, tato skutečnost musí být doložena potvrzením organizační složky výrobce v ČR. Potvrzení musí být v českém jazyce a musí být vytvořena výhradně pro účely tohoto VŘ.

Pokročilá ochrana koncových bodů

Zadavatel požaduje zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux a mobilních zařízení s OS Android a iOS. Zadavatel požaduje dodávku 150 Ks licencí na 5 let.

Požadované parametry:

Konzole pro centrální správu řešení
Všechny komponenty řešení musejí být v českém jazyce – včetně konzole správy, klientské aplikace a manuálů
Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí
Možnost kdykoli zmigrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení
Konzole pro centrální správu je kompletně multi-tenantní
Základní vlastnosti
Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu
Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem
Možnost zasílat upozornění napojením na Syslog server

Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce
Úlohy správy bezpečnosti
Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.
Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery
Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity
Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy
Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy
Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy
Centralizované místo pro záznam všech úloh
Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)
Nastavení úrovně bezpečnosti
Více možností přiřazení pravidel: podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD
Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně dle sekcí a subsekcí nastavení bezpečnostních pravidel
Reportování
Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě
Možnost zasílání vygenerovaných reportů e-mailem
Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv
Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen
Karanténa
Vzdálená obnova či smazání souboru v karanténě.

Možnost automaticky přidat soubor do výjimky při obnově z karantény
Uživatelé
Musí umožňovat RBAC s podporou 2-faktorového ověření a možnost jeho vynucení
Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny
Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení. Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat
Logy
Zaznamenávání uživatelských akcí do logu s detailním rozspisem každé akce včetně vyhledávání
Správa a instalace ochrany
Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány
Instalace může být provedena několika způsoby, alespoň: 1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován 2. Instalace vzdáleně přímo z konzole správy 3. Distribuce instalačního balíčku pomocí GPO či SCCM
Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN
Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou
Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci
Konzole správy obsahuje detailní informace o chráněných strojích: mimo jiné název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích
Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů
Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou
Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti
Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)
Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body
Možnost spustit Network discovery z kteréhokoli již instalovaného klienta

Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):
- Podpora operačních systémů: Windows 10 1507 a vyšší, Windows 8.1, Windows 10 Enterprise, - Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, - Ubuntu 14.04 LTS a vyšší - Red Hat Enterprise Linux - CentOS 6.0 a vyšší - SUSE Linux Enterprise Server 11 SP4 a vyšší - Mac OS X El Capitan (10.11) a vyšší
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů, může být omezeno veliksotí souboru,
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
Detekce na základě virových definicí (tzn. signatur)
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
Detekce 0-day útoků na základě odhalování anomálního chování
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
Detekce 0-day bezsouborových útoků
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně

Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
Možnost automatické detonace podezřelých souborů v Sandboxu
Možnost nastavení Sandboxu – délka pozorování po spuštění, počet opakování spuštění, přístup k internetu během spuštění ano i ne
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
Možnost ručního vložení vzorku do Sandboxu
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy
Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
Řešení umožňuje analýzu vektoru útoku
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní
Možnost prověřovat http provoz
Možnost prověřovat provoz šifrovaný pomocí SSL
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic
Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)

Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
Ochrana proti podvodným a phishingovým webovým stránkám
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
Možnost rozšíření o správu patchů aplikací třetích stran
Možnost rozšíření o správu šifrování pevných disků
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)
Firewall
Možnost blokovat skenování portů
Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS
Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb
Možnost vypnout IDS
Možnost nastavit profily známých sítí
Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu
Karanténa
Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě
Možnost obnovy souboru do originální či do nově zadané lokality
Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní)
Kontrola přístupu k internetu
• Zablokování přístupu na internet pro specifické stanice / skupiny stanic • Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic • Zablokování přístupu k internetu v určený čas • Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné) • Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)

Ochrana virtualizovaných koncových bodů (Windows, Linux)
Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením ; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen
„Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením
„Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže
Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení
Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace)
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
Detekce na základě virových definicí (tzn. signatur)
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
Detekce 0-day útoků na základě odhalování anomálního chování
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
Detekce 0-day bezsouborových útoků

Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
Možnost automatické detonace podezřelých souborů v Sandboxu
Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
Možnost ručního vložení vzorku do Sandboxu
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy
Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
Řešení umožňuje analýzu vektoru útoku
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
Možnost prověřovat http provoz
Možnost prověřovat provoz šifrovaný pomocí SSL

Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic
Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
Ochrana proti podvodným a phishingovým webovým stránkám
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)

Zero Client 20 ks

Požadované parametry:

Požadované parametry zero client
Zerocliet s hliníkovým tělem a max. rozměry 10,5 CM x 9,5 CM x 4 CM, musí umožňovat kombinaci aktivního i neaktivního chlazení, disponovat vypínacím tlačítkem,
CPU min. 4 Core, 1500 MHz
RAM min 4GB DDR4
Podpora 4K grafického zobrazení a dvou monitorů.
Musí disponovat min. 2 x HDMI, 4 x USB (Z toho 2 x USB 3.0) , Bluetooth 5.0, 3,5 mm jack, Micro SD Slot osazen min 16GB
Možnost rozšíření o M.2 Kartu
Zdroj součásti dodávky min 3A
Operační sytém podporující RDS, Blast, PCoIP, Citrix, který je hardenizovaný proti napadení kybernetickým útokem.
Musí podporovat centrální management, kdy je možné distribuovat FW, Konfigurace, Certifikáty a práva z jednoho místa přes grafické rozhraní
Musí podpora automatické nasazení klienta
Musí podporavat celtrální logování do management nástroje pro tenké klienty
Podpora NBD na 5 let od výrobce zařízení

Služby požadované spolu s plněním

Pro část plnění: Server s grafickým adaptérem

- Doprava a montáže serveru
- Instlalace a konfigurace ESXi
- Začlenění do již provozovaného clusteru
- Sestavení VSAN Clusteru
- Migrace VM ze stávajícího datového uložiště
- Aktualizace kompleního VMware Clusteru včetně vCenter a vDSwicth

- Aktualizace VMware Horizon prostředí
- Bezplatný dohled po dobu 90 dní na dodanou infrasturkutou a řešení závad formou reklamace
- Demonstrace funkčnosti
- Akceptace formou akceptačních testů, dle požadavků zadavatele
- Zaškolení správců v rozsahu 8 hodin

Pro část plnění:. Pokročilá ochrana koncových bodů

- Odinstalace původního řešení
- Implementace cetrální konzole pro správu řešení
- Navržení bezpečnostních politik pro každou skupinu uživatelů a serverů
- Deployment koncového řešení pro Servery
- Deployment koncového řešení pro Stanice
- Bezplatný dohled po dobu 90 dní na dodánou infrasturkutou a řešení závad
- Demonstrace funkčnosti
- Akceptace formou akceptačních testů, dle požadavků zavatele
- Zaškolení správců v rozsahu 8 hodin

Pro část plnění:. Zero Client

- Kompletní implemetace všech ks Zero Client
- Nasazení centrálního managementu
- Vytvoření konfiguračních profile pro jednotlivé úseky
- Implemetace řešení pro přechod na tenké klienty

Rozšířená diagnostika VMware prostředí

Zadavatel požaduje po instalaci udělat rozšířenou diagnostiku prostředí VMware, kdy bude vyžadovat výstupní dokumentaci.

Zadavatel požaduje provedení služby analýzy prostředí VMware v rozsahu:

- VMware Check
- Performance a HW Check
- Synergie komponent
- Výstupní dokumentace

Analýza VMware prostředí bude obsahovat:

- Analýza bude provedena pomocí nástrojů výrobce k tomu určených, nepřipouští se řešení vlastní, ani řešení třetích stran.
- Analýza použitých komponent a využitých firmware v kontextu provozovaného prostředí VMware.
- Revize konfigurace s ohledem na Best practice výrobce
- Každé ze zjištění bude mít rozepsaný kompletní dopad nálezu na dostupnost či výkon prostředí
- Všechna zjištění budou kategorizována dle závažnosti do 4 kategorií
- Ve výstupní dokumetaci budou jenotlivá zjištění rozepsána a bude k nim uveden komentář proč je zjištění závadné jak jej uvést do korektního stavu.
- Tyto zjištění a komentáře budou rozvedena na min. dvou wokshopech společně s odpovědnými osobami zadavatele.

- Výsledkem bude dokumetnace, kde budou všechny tyto zjiště sepsány, včetně komentářu a popisu naimplementovaných změn
- Dokuemtace bude před odevzdáním odsouhlasena zadavatelem.

Analyzované prostředí:

Data Center	1
Cluster	1
ESXi Server	4
Virtual Machine	155