ÚVN-VoFN Praha - kybernetická bezpečnost_monitoring - nákup - software - část 1 SABRA

Název dodavatele: Thein Security s.r.o.
IČO: 27415546
Jméno osoby odpovědné za podanou nabídku: [redacted]
E-mail odpovědné osoby: [redacted]
Výrobce nabízeného řešení: Palo Alto Networks / Cortex XSIAM

bod	Minimální požadované technické parametry na XDR řešení:	Splňuje požadovaný parametr: (ANO/NE) V případě, že účastník doplní ne, znamená to nesplnění minimálních technických podmínek a bude vyloučen	Způsob (případné licence) jakým je uvedený parametr naplněn a kde může, doplní účastník odkaz na dokumentaci výrobce, apod.
1	**Obecné požadavky:**		
2	Všechny požadované funkce týkající se koncového bodu, jakými jsou zejména, ale nikoliv výlučně ochrana před nákezou, sběr dat k analýze, zajištění shody s pravidly (compliance), jsou prováděny výhradně jediným agentem běžícím na koncovém bodě.	[redacted]	
3	Všechny úkony týkající se zejména, ale nikoliv výlučně konfigurace systému, správy a ochrany koncových zařízení, forenzní analýzy jsou prováděny v jednotné konzoli, přístupné pomocí webového rozhraní.		
4	Dodávaný systém umožňuje správu koncových zařízení, která nedisponují přímou konektivitou do internetu. K tomu je možno použít on-premise virtuální server, sloužící jako proxy pro komunikaci s managementem , a který je zahrnut v ceně dodávaného systému, nebo je jeho použití bezplatné. Výpočetní prostředky nutné pro jeho běh jsou dodávány zadavatelem.		
5	Dodávaný systém musí umožnit volitelné rozšíření o funkci pro sběr dat z on-premise zdrojů, jako jsou Windows event logy, syslog, netflow apod. K zaslání těchto logů do centrálního úložiště je možno použít on-premise virtuální server, který je zahrnut v ceně dodávaného systému, nebo je jeho použití bezplatné. Výpočetní prostředky nutné pro jeho běh jsou dodávány zadavatelem.		
6	Dodávaný systém zajišťuje sběr takových dat z koncových zařízení, která jsou relevantní k zastavení nebo detekci útoku a následné forenzní analýze.		
7	Dodávaný systém musí umožnit volitelné rozšíření o funkci pro detekci a prevenci bezpečnostních incidentů pro data zejména, nikoliv výlučně z následujících zdrojů: Netflow, firewallové logy nezávislé na výrobci FW, Windows Event logy.		
8	Dodávaný systém umožňuje napojení na zdroje identit minimálně následujících typů: Entra ID, on-premise AD, Okta. Tato data jsou určena pro obohacení detekčních schopností systému.		
9	Dodávaný systém spravuje administrátorské účty interně, nebo používá identity uložené u jakéhokoliv IdP pomocí protokolu SAML.Všechny varianty musí podporovat MFA.		
10	Dodávaný systém umožňuje segregaci rolí tak, že jednotlivým správcům zpřístupní pouze vybrané funkcionality systému.		
11	Dodávaný systém umožňuje segregaci rolí tak, že jednotlivým správcům umožní spravovat pouze vybrané skupiny koncových zařízení.		
12	Dodávaný systém umožňuje segregaci rolí tak, že jednotlivým správcům umožní přistupovat pouze k těm datům v systému, ke kterým je mu udělen přístup.		
13	Dodávaný systém obsahuje možnost zapnout multifaktorovou autentizaci pro správce bez nutnosti poskytnout toto řešení ze strany zákazníka.		
14	Dodávaný systém obsahuje API pro umožnění integrace nástrojů třetích stran a pro provádění administrativních úkonů.		
15	Dodávaný systém umožňuje export dat ve formátu syslog pro nástroj správy logů třetí strany.		
16	Dodávaný systém umožňuje tvorbu dynamických dashboardů, čerpající data definovaná libovolným uživatelským pohledem do báze dat.		
17	Data jsou uchována výhradně v rámci EU.		
18	Data jsou uchována výhradně v datových centrech certifikovaných na SOC2 Type II+.		
19	Výrobce dodávající systém má platnou certifikaci ISO 27001.		
20	Dodávaný systém umožňuje použít vlastní šifrovací klíče pro zabezpečení sebraných dat.		
21	Dodávaný systém licenčně neomezuje množství dat, sebraných z koncových bodů agentem systému.		
22	Dodávaný systém umožňuje zpracovávat 100 GB dat třetích stran (např. dat z autentizačních služeb, firewallů apod.) denně.		

23	Všechny události (nejen alerty a k nim přidružené informace) v maximálním detailu jsou uchovávány po dobu minimálně třiceti dnů, s možností prodloužení v hot, nebo cold storage.
24	**Zajištění visibility:**
25	Dodávaný systém získává pro analýzu uživatelská data (doménové jméno, organizační složka, email adresa, typické koncové zařízení, uživatel spouštějící proces) napojením na interní adresářovou službu.
26	Dodávaný systém získává pro analýzu informace o koncovém zařízení (IP adresa, MAC adresa, název a doména, informace o OS, informace o instalovaném SW) prostřednictvím agenta nainstalovaného na koncovém zařízení.
27	Dodávaný systém získává pro analýzu informace o procesu (časové razítko, cesta a jméno, ID procesu, hash MD5 nebo SHA-256, parametry) spouštěném na koncovém zařízení, pomocí agenta, který je na koncovém zařízení nainstalován.
28	Dodávaný systém získává pro analýzu informace o souborech (časové razítko, cesta a jméno, historie umístění a jména, hash MD5 nebo SHA-256) a práci s nimi (vytvoření, smazání, přejmenování, přesun, zkopírování) prostřednictvím agenta nainstalovaného na koncovém zařízení.
29	Dodávaný systém získává pro analýzu informace o registrech systémů Windows (časové razítko, název zápisu, jeho hodnota a typ, historie změn) prostřednictvím agenta nainstalovaného na koncovém zařízení.
30	Dodávaný systém získává pro analýzu informace o systémových událostech, jako je zejména, nikoliv však výlučně přihlášení a odhlášení uživatele prostřednictvím agenta nainstalovaného na koncovém zařízení.
31	Dodávaný systém musí umožnit doplnění dat z koncových zařízení k bezpečnostním událostem získaným z dalších zařízení (funkce XDR), jakými jsou mimo jiné IPS, firewally nové generace, aplikační firewally apod.
32	Dodávaný systém musí umožnit volitelné rozšíření umožňující získání informace pro analýzu ze síťových prvků (časové razítko, zdrojová a cílová IP adresa i port, přenesený objem dat, protokol, geolokační data, integrace s aplikačním firewallem pro kompletní analýzu layer 7 včetně jména aplikace, doba spojení, rozšířená data o klíčových protokolech - DNS, HTTP, DHCP, RPC, ICMP, ARP). K tomu musí být schopen použít stávající síťová zařízení instalovaná v síti zákazníka. Podpora minimálně firewallů nové generace výrobců Cisco, Fortinet, Checkpoint, Palo Alto Networks.
33	**Snížení plochy pro útok:**
34	Dodávaný systém umožňuje omezit sadu souborů, které je možné na dané koncové stanici spustit na soubory předem definované prostřednictvím tzv. allow listu nebo block listu na základě hash hodnoty, umístění a digitálního podpisu souboru.
35	Dodávaný systém umožňuje zakázat spouštění souborů z administrátorem definovaných lokací (síťová úložiště, stažené soubory apod.).
36	Dodávaný systém umožňuje zakázat spouštění souborů, které nejsou podepsané důvěryhodným vydavatelem.
37	Dodávaný systém umožňuje vynutit a ověřit šifrování disku koncového zařízení minimálně pro systémy Windows a MacOS.
38	Dodávaný systém umožňuje nastavit pravidla lokálního firewallu koncového zařízení minimálně pro systémy Windows a MacOS.
39	Dodávaný systém poskytuje informace o zranitelnostech koncového zařízení.
40	Dodávaný systém poskytuje informace o HW a operačním systému koncového zařízení.
41	Dodávaný systém poskytuje informace o aplikacích nainstalovaných na koncovém zařízení.
42	Dodávaný systém poskytuje informace o lokálních účtech, sdílených discích a příslušnosti lokálních účtů ke skupinám, např. pro možnost identifikace lokálních administrátorů koncových zařízení.
43	Dodávaný systém umožňuje řízení využití portů USB, jakými jsou nejen přenosná úložiště, ale i další libovolná USB zařízení, včetně možnosti povolit či zakázat pouze specifický typ zařízení/výrobce.
44	Dodávaný systém umožňuje řízení bluetooth zařízení, včetně možnosti povolit či zakázat pouze specifický typ zařízení/výrobce.
45	Dodávaný systém poskytuje možnost skenování koncových stanic za účelem nalezení malware dle plánu či na vyžádání.
46	Dodávaný systém zajišťuje správu koncových zařízení i za účelem identifikace cizích zařízení, nabízí tedy tzv. asset management.
47	**Prevence útoků:**
48	Dodávaný systém provádí kontrolu procesu již před jeho spuštěním a na základě reputace souboru povolí, nebo zakáže jeho spuštění.
49	Dodávaný systém poskytuje funkci povolení spuštění pouze známých neškodných souborů a zákazu všech ostatních (neznámých, či škodlivých) a to i bez přístupu k internetu.
50	Dodávaný systém poskytuje ochranu před známým škodlivým kódem i bez nutnosti pravidelné aktualizace databáze signatur.

51	Dodávaný systém poskytuje ochranu před známým i neznámým škodlivým kódem i bez nutnosti být v tu chvíli připojen k internetu či interní síti.	[redacted]
52	Dodávaný systém brání spuštění škodlivých procesů, stejně jako činnosti, která je vyhodnocena jako škodlivá až v průběhu běhu procesu.	
53	Dodávaný systém brání škodlivému chování, které je způsobeno legitimními procesy.	
54	Dodávaný systém poskytuje ochranu před bezsouborovými útoky.	
55	Dodávaný systém provádí dynamickou analýzu chování běžících procesů.	
56	Dodávaný systém obsahuje funkci dynamické analýzy v sandboxu, včetně doručení reportu, popisujícího chování souboru.	
57	Dodávaný systém poskytuje funkci sandboxu, zajišťující dynamickou analýzu spustitelných souborů pro operační systémy Windows, MacOS, Android a Linux. Tento sandbox je součástí poskytovaného řešení.	
58	Dodávaný systém poskytuje dynamickou analýzu dat v sandboxu, jak s využitím virtuálního, tak bare-metal prostředí pro zabránění evazivnímu chování škodlivého kódu.	
59	Dodávaný systém dokáže zastavit spuštění neznámého souboru, dokud nezíská verdikt z dynamické analýzy sandboxu.	
60	Dodávaný systém umožňuje manuální změnu verdiktu poskytnutého dynamickou analýzou.	
61	Dodávaný systém odesílá vzorky k analýze do sandboxu na základě hash hodnot. Jeden identický soubor tak není analyzován zbytečně vícekrát, byť má rozdílný název.	
62	Dodávaný systém obsahuje funkci lokální analýzy, využívající prvky strojového učení.	
63	Dodávaný systém umožňuje vytvoření pravidel/zásad, které zamezí konkrétním scénářům spuštění škodlivého kódu.	
64	Dodávaný systém poskytuje ochranu před útokem pomocí manipulace s pamětí a spuštěním kódu z datové oblasti (techniky DEP, JIT, ROP).	
65	Dodávaný systém umožňuje blokaci útočných technik jakými je například vkládání kódu.	
66	Dodávaný systém umožňuje blokaci DLL knihoven s nebezpečným umístěním.	
67	Dodávaný systém umožňuje blokaci útočných technik manipulujících s obsahem (heap spray, buffer overflow apod.).	
68	Dodávaný systém umožňuje kontrolu síťového provozu a blokaci škodlivé komunikace.	
69	Dodávaný systém umožňuje tvorbu uživatelem definovaných pravidel pro blokaci specifických hrozeb.	
70	**Detekce pokročilých hrozeb (APT):**	
71	Dodávaný systém používá k detekci hrozeb vytvoření standardního chování síťového provozu, uživatelů, i konkrétních koncových zařízení (tzv. baseline) a sleduje odchylky zachycené systémem strojového učení.	
72	Dodávaný systém provádí detekci anomálií síťového provozu a chování známých procesů nejen na základě baseline vytvořené v prostředí dané organizace, ale i srovnáním s běžným chováním dalších organizací ve světě.	
73	Dodávaný systém provádí detekci hrozeb na základě pravidel definovaných výrobcem, založených na základě chování, které je při útocích využíváno (TTP MITRE ATT&CK).	
74	Dodávaný systém umožňuje tvorbu uživatelských IOC na základě zadání celé cesty umístění souboru, jména souboru, navštěvované domény, IP adresy, hashe souboru, nebo pokročilé behaviorální IOC skládající se z řetězce událostí jako je např. vytváření souborů, spouštění specifických procesů, úprav registrů, iniciace síťové komunikace.	
75	Dodávaný systém umožňuje přebírání informací o nových hrozbách ze zdrojů třetích stran ve formátu JSON a CSV.	

76	Dodávaný systém umožňuje vytváření IOC pomocí API, včetně možnosti importu více IOC najednou a importu IOC z CSV souboru v konzoli pro správu.	
77	Dodávaný systém umožňuje nastavit pro jednotlivé IOC hodnotu závažnosti.	
78	Dodávaný systém umožňuje tvorbu korelačních pravidel napříč daty v něm uloženými, nezávisle na tom, jestli se jedná o data, která byla nativně systémem vytvořena, nebo o data ze zdrojů třetích stran, která byla do systému přeposlána.	
79	**Dodávaný systém detekuje minimálně následující události:**	
80	Nestandardní síťová komunikace, jako je neúspěšná komunikace, změna v objemu z pohledu množství dat, nebo relací, první úspěšné přihlášení z nové země, přihlášení jedním účtem z více zemí v krátkém časovém úseku, administrátorská komunikace ze stanice, která byla dříve pouze uživatelskou, neočekávaná SMTP a SSH spojení.	
81	Spuštění nové služby, která neodpovídá charakteru koncového zařízení.	
82	Nestandardní uživatelské chování, které je v rozporu s charakterem ostatních typových koncových zařízení, nestandardní komunikace známých procesů, spuštění známých zneužitelných procesů např. z dokumentů MS Office.	
83	Nestandardní práce s uživatelskými účty, jako jsou výjimečná přihlášení výchozími účty, snaha o přihlášení zablokovaným účtem, nebo účtem, který nebyl dlouho použit, neúspěšná snaha o přihlášení stejným účtem na více koncových zařízeních, snaha o získání uložených přihlašovacích údajů (mimikatz, cmdkey), výjimečný přístup k datům, nestandardní chování interního uživatele, nestandardní modifikace oprávnění účtu, exfiltrace dat na fyzická úložiště apod.	
84	Dodávaný systém musí umožnit volitelné rozšíření o detekci nestandardního DNS chování, jako je DNS tunneling, více neúspěšných DNS dotazů.	
86	Nestandardní práce se soubory, jako je např. zpožděné smazání, závislé na ověření konkrétní komunikace.	
86	Skenování okolních počítačů, ať již pomocí standardních port či sweep skenů, nebo použití WMIC.	
87	Snaha o prolomení hesel, jako je bruteforce útok.	
88	Chování, odpovídající známé útočné technice.	
89	Analýza PowerShell skriptů pomocí analytiky založené na AI.	
90	**Reakce na hrozby:**	
91	Dodávaný systém umožňuje v reakci na detekci bezpečnostní události spustit sken vzdáleného počítače pro nalezení dalšího škodlivého software	
92	Dodávaný systém umožňuje zabezpečený a logovaný terminálový přístup na koncovou stanici. Tento vzdálený přístup musí být možné pro kritické cíle možno nevratně vypnout.	
93	Dodávaný systém umožňuje v reakci na zaznamenanou hrozbu, nebo i manuálně spustit skript či příkaz v prostředí Windows (CMD, PowerShell, Python) a skripty typu bash a Python v prostředí MacOSX a Linux.	
94	Dodávaný systém umožňuje spuštění Python skriptu na více koncových zařízeních nezávisle na jejich OS (Windows, macOS, Linux) a bez nutnosti instalovat prostředí Python. Skript je interpretován součástí agenta nainstalovaného na koncovém zařízení.	
95	Dodávaný systém obsahuje předdefinovanou sadu skriptů pro snadný sběr dat, jejich analýzu a vyhodnocení, stejně jako pro servisní zásahy okamžitě blokující útok probíhající na koncovém zařízení.	
96	Dodávaný systém umožňuje automaticky izolovat jedno či více nakažených koncových zařízení tak, že koncové zařízení má možnost komunikovat pouze s managementem dodávaného systému, nebo s cíli, definovanými administrátorem systému.	
97	Dodávaný systém musí umožnit funkci pro vzdálené smazání podezřelého či škodlivého souboru z jednoho či více koncových zařízení najednou pomocí grafického rozhraní i pomocí skriptu.	
98	Dodávaný systém musí umožnit spustit výše uvedené akce manuálně, nebo na základě detekce specifické události.	
99	Dodávaný systém musí poskytnout automatizovaný návrat do stavu před incidentem, nebo popis postupu, jak se do takového stavu dostat.	
100	**Analýza incidentů a vyšetřování:**	

101	Dodávaný systém poskytuje automatizovanou analýzu hlavní příčiny jakéhokoliv incidentu, včetně nástrojů a dat pro detailní forenzní analýzu.	
102	Dodávaný systém provádí vizualizaci jednotlivých kroků tvořících incident, včetně možnosti přehledně sledovat jejich časovou posloupnost, včetně současného výskytu na dalších koncových zařízeních.	
103	Dodávaný systém poskytuje nástroj pro vyhledávání ve všech nasbíraných datech pomocí plnohodnotného dotazovacího jazyka. Tento nástroj zajistí možnost vyhledat jakoukoliv uloženou informaci.	
104	Dodávaný systém poskytuje uživatelsky přívětivý nástroj pro vyhledávání v nasbíraných datech pomocí grafického rozhraní správcovské konzole.	
105	Dodávaný systém v rámci incidentu automaticky propojí a přehledně prezentuje informace ze všech zdrojů dat, vztahující se k detekovanému incidentu.	
106	Dodávaný systém prezentuje všechny akce a incidenty na časové ose.	
107	Dodávaný systém prezentuje informaci o tom, jestli byla škodlivá činnost blokována agentem na koncovém bodu, firewallem, nebo jinou preventivní technologií.	
108	Dodávaný systém poskytuje pouze relevantní informace a potlačuje šum, např. odstranění bezvýznamných binárních souborů a DLL knihoven z řetězce událostí. Tyto potlačené informace, které nejsou relevantní k vyšetřování incidentu je však stále možno dohledat.	
109	Dodávaný systém umožňuje vyhledávat indikátory kompromitace napříč jednotlivými koncovými zařízeními, např. v případě výskytu škodlivého souboru na jednom z koncových zařízení je možné automaticky prohledat, jestli se tento soubor nevyskytuje i na dalších spravovaných koncových zařízeních, nebo při výskytu škodlivé komunikace je možno vyhledat, která koncová zařízení (i ta bez nainstalovaného agenta) komunikovala obdobně.	
110	Dodávaný systém poskytuje funkci zpětného vyhledávání v historických datech. Ve chvíli, kdy je vytvořen či výrobcem doplněn nový IOC nebo BIOC, je systém schopen prohledat dostupná historická data a vytvořit incidenty, ke kterým došlo v minulosti, kdy ještě konkrétní způsob útoku nebyl známý.	
111	Dodávaný systém poskytuje funkci řízeného vyhledávání hrozeb na základě IOC pro snadné a rychlé prověření celého prostředí.	
112	Dodávaný systém zobrazuje u každé části incidentu její návaznosti na standardizovaný framework MITRE ATT&CK.	
113	Dodávaný systém obsahuje integrovanou MITRE ATT&CK matici s vyznačenými technikami, které daná část útoku používá.	
114	Dodávaný systém umožňuje tvorbu vlastních pravidel, které definují skóre jednotlivých incidentů pro účely jejich prioritizace.	
115	Dodávaný systém umožňuje sběr dat pro forenzní analýzu i ze zařízení, která jsou kompletně odpojena z datové sítě.	
116	Dodávaný systém umožňuje stažení aktuálního obsahu operační paměti.	
117	Dodávaný systém umožňuje sběr forenzních dat nejen po vzniku incidentu, ale i v průběhu běžné činnosti koncové stanice. Je tak možné srovnání stavu před a po vzniku incidentu.	
118	**Forenzní analýza:**	
119	Automatizovaný sběr forenzních dat z koncového zařízení (minimálně procesy, síťová spojení, registr, soubory, služby, přihlášení, kompletní obsah operační paměti).	
120	Možnost dálkového spuštění sběru forenzních dat bez fyzického přístupu ke stanici.	
121	Provádění forenzní analýzy bez narušení činnosti uživatele (stealth mode).	
122	Předdefinované šablony sběru dat dle typu incidentu nebo podezřelého chování.	
123	Centralizované zobrazení výsledků s možností filtrování, porovnání a časové analýzy.	
124	Analýza artefaktů v kontextu bezpečnostního incidentu.	
125	Retence forenzních dat po dobu minimálně 30 dní.	
126	Možnost exportu výsledků do standardních formátů (např. JSON, CSV, PDF).	
127	Integrace s dalšími moduly platformy (např. incident management, threat intelligence).	
128	Správa modulu z centrální platformy/kontrolní konzole.	

129	Šifrovaná komunikace mezi koncovým bodem a centrální platformou.	
130	Auditovatelnost všech provedených forenzních operací.	
131	Možnost licencování dle počtu koncových zařízení.	
132	**Správa incidentů:**	
133	Dodávaný systém poskytuje funkci incident managementu pro události detekované systémem, stejně jako pro události detekované jinými systémy v rámci XDR (IPS, firewally apod.)	
134	Dodávaný systém udržuje životní cyklus incidentu, jako je jeho otevření, přiřazení řešiteli, vyšetření, uzavření.	
135	Dodávaný systém automaticky seskupuje související události do jednoho incidentu.	
136	Dodávaný systém umožňuje manuální přepsání závažnosti incidentu.	
137	Dodávaný systém poskytuje informaci o všech uživatelích, zařízení, souborech a doménách zapojených do konkrétního incidentu.	
138	Dodávaný systém umožňuje manuální sloučení incidentů.	
139	Dodávaný systém umožňuje přiřadit incident konkrétnímu řešiteli, včetně zaslání notifikace.	
140	Dodávaný systém umožňuje přiřadit incidentu komentáře.	
141	Dodávaný systém umožňuje exportovat informaci o incidentu do nástrojů třetích stran.	
142	**Parametry a správa agenta koncových zařízení:**	
143	Agent instalovaný na koncové zařízení zásadně neovlivní jeho výkon pro běžnou činnost.	
144	Agent nainstalovaný na koncovém zařízení žádným způsobem nenarušuje činnost VPN agentů Anyconnect a GlobalProtect používaných zákazníkem.	
145	Dodávaný systém zaručuje, že koncoví uživatelé nejsou schopni obejít bezpečnostní pravidla, i když mají práva místních správců.	
146	Dodávaný systém zaručuje, že agenta není z koncového zařízení možné odinstalovat/odstranit bez znalosti časově omezeného tokenu.	
147	Dodávaný systém zaručuje, že ani lokální administrátoři nemohou zastavit agenta nebo související služby.	
148	Dodávaný systém zaručuje, že ani lokální administrátoři nemohou upravit součásti systému ochrany koncových zařízení, programové složky a záznamy v registru, které jsou potřebné pro plnohodnotnou ochranu.	
149	Dodávaný systém zaručuje, že agenta je možno aktualizovat z prostředí centrálního managementu.	
150	Dodávaný systém zaručuje podporu provozu v non-persistentním VDI prostředí	
151	Agent je možno nainstalovat minimálně na následující platformy a OS:	
152	Všechny aktuálně podporované verze Microsoft Windows (32-bit, 64-bit)	
153	Všechny aktuálně podporované verze Microsoft Windows Server (32-bit, 64-bit)	
154	Všechny enterprise distribuce Linux (Debian, Ubuntu, Red Hat, SuSE Linux Enterprise server, CentOS, AlmaLinux, Oracle Linux, Rocky Linux, Amazon Linux)	

155	Všechny aktuálně podporované verze Apple MAC OS a MAC OS X – min. Catalina a novější včetně Sequoia	
156	Apple iOS 15 a novější	
157	Citrix XenDesktop RDS + VDI, XenApp	
158	VMware Horizon View, Appvolumes, ThinApp	
159	Android OS 10 a novější	
160	Dodávaný systém je plnohodnotnou náhradou antivirového řešení a systém Microsoft Windows ho tak ve svém system centru zobrazuje.	
161	Dodávaný systém zaručuje, že agent pro operační systém Linux poskytuje možnost využití user space, pokud není možné použít kernel mode.	
162	**Integrace s dalšími systémy:**	
163	Dodávaný systém bude dodavatelem integrován s používanými firewally (Checkpoint) tak, aby byly firewally automaticky a okamžitě po získání informace schopny blokovat IP adresy či domény označené dodávaným systémem jako nevhodné.	
164	Dodávaný systém musí umožnit příjetí událostí z IPS používaného firewallu (Checkpoint) a obohatit tuto událost o data z koncových stanic tak, aby bylo ihned zřejmé, jaká stanice, uživatel a posloupnost procesů stála za vznikem detekované události.	
165	Dodávaný systém musí umožňovat odesílání detekovaných událostí do platformy SIEM, hostované v prostředí Zadavatele.	
166	Dodávaný systém umožňuje integraci se SOAR řešením pro analýzu incidentů, hostovaným v prostředí Zadavatele	
167	Dodávaný systém umožňuje integraci se systémy Threat Intel, jako např. Virus Total	
168	Dodávaný systém umožňuje nativní integraci a sběr logů z AWS, Azure, GoogleCloud	
169	Dodávaný systém umožňuje nativní integraci a sběr logů z vulnerability nástrojů Rapid7 InsightVM a Tenable	
170	Dodávaný systém umožňuje nativní integraci a sběr logů z O365/M365	
171	**Automatizované funkcionality - Security Orchestration, Automation & Response (SOAR)**	
172	Dodávaný systém musí obsahovat integrovaný nástroj pro automatizaci a orchestraci bezpečnostních incidentů (SOAR), který je součástí nabídky bez potřeby použití produktů třetích stran.	
173	Dodávaný systém musí obsahovat grafický editor playbooků (automatizačních scénářů) s možností větvení, podmínek, paralelizace úloh a rozhraním „drag & drop“.	
174	Dodávaný systém musí umožnit automatizované vyšetřování incidentů, včetně interakce s externími systémy (např. Active Directory, firewall, e-mailové brány) bez nutnosti psaní vlastního kódu.	
175	Dodávaný systém umožňuje automatizaci rutinních bezpečnostních operací (např. blokování IP adres, izolace endpointů).	
176	Dodávaný systém umožňuje orchestraci procesů mezi různými bezpečnostními technologiemi (SIEM, EDR, Threat Intelligence, NGFW)	
177	Dodávaný systém umožňuje podporu tvorby a úpravy playbooků pro reakci na incidenty standardizovaným způsobem.	
178	Dodávaný systém umožňuje shromažďování, centralizaci zpracování bezpečnostních událostí a následný case management bezpečnostních incidentů.	
179	Dodávaný systém umožňuje podporu workflow pro eskalaci a řešení bezpečnostních incidentů.	

180	Dodávaný systém umožňuje přidělování incidentů/úkolů členům bezpečnostního týmu.	
181	Dodávaný systém podporuje integraci s Threat Intelligence Feeds pro obohacení detekce hrozeb.	
182	Dodávaný systém umožňuje automatizované vyhodnocení indikátorů kompromitace (IOC)	
183	Dodávaný systém umožňuje využití API pro integraci s dalšími bezpečnostními nástroji.	
184	Dodávaný systém umožňuje rozšíření funkcionelit pomocí vlastních skriptů a konektorů.	
185	Dodávaný systém obsahuje Marketplace s již existujícími integracemi na 3rd party zdroje dat., integrace pro umožnění response akcí.	
186	Dodávaný systém umožňuje generování dashboardů a reportů o incidentech. SLA	
187	Dodávaný systém obsahuje auditní stopu pro všechny provedené akce	
188	**Automatizované funkcionality - Threat Intelligence Platform (TIP)**	
189	Dodávaný systém obsahuje modul pro funkcionalitu TIP - Threat Intelligence Platform	
190	Dodávaný systém musí obsahovat minimálně jeden komerční feed Threat Intelligence zdroje.	
191	Dodávaný systém umožňuje automatizované shromažďování dat z více Threat Intelligence zdrojů (open-source, komerční, komunitní, vlastní).	
192	Dodávaný systém podporuje integraci s externími Threat Intelligence feedy a databázemi (STIX/TAXII, MISP, VirusTotal, atd.).	
193	Dodávaný systém musí mít integrovanou Threat Intelligence platformu s možností správy, deduplikace a automatického enrichmentu IOCs z více externích zdrojů.	
194	Dodávaný systém musí umožnit automatické mapování indikátorů hrozeb (IOCs) na MITRE ATT&CK techniky a korelaci s reálnými událostmi v systému.	
195	Dodávaný systém musí podporovat vytváření vlastních intel feedů a jejich distribuci do ostatních bezpečnostních nástrojů (např. SIEM, EDR, FW).	
196	Dodávaný systém obsahuje mechanismy pro obohacování hrozeb kontextovými informacemi (geolokace, WHOIS, reputace, CVE, MITRE ATT&CK).	
197	Dodávaný systém umožňuje deduplikaci, normalizaci a prioritizaci Threat Intelligence dat.	
198	Dodávaný systém obsahuje engine pro korelaci hrozeb napříč různými zdroji dat.	
199	Dodávaný systém umožňuje mapování zjištěných indikátorů kompromitace (IOC) na rámce jako MITRE ATT&CK, Cyber Kill Chain a další.	
200	Dodávaný systém podporuje automatizované skórování IOC na základě důvěryhodnosti zdrojů a kontextu hrozby.	
201	Dodávaný systém umožňuje vizualizaci vztahů mezi hrozbami (graph-based analysis, entity linking).	
202	Dodávaný systém umožňuje automatizované enrichment IOC pomocí připojených Threat Intelligence zdrojů.	

203	Dodávaný systém podporuje tvorbu a spouštění playbooků na základě korelace hrozeb.	[redacted]

Netechnické požadavky
Pokud je u splnění požadavku uvedeno ANO, musí být případná potřebná licence na celou dobu trvání podpory součástí dodávky