2 Technická specifikace

Předmětem nabídky je zabezpečení koncových bodů proti Zero-day útokům řešením Trend Micro. Nabízené řešení bude nasazeno na 800 kusů koncových zařízení s aktualizací na dobu 12 měsíců.

Nabízené řešení splňuje všechny požadavky zadavatele.

	Obecné	
1	Podporované operační systémy Windows 7, Windows Server 2008R2, SUSE Enterprise Server 12, Redhat, Ubuntu, CentOS, Amazon, Oracle. Včetně jejich novějších verzí.	Ano
2	Malý dopad na zdroje koncového zařízení jako jsou CPU (max 20%), operační paměť (max 250MB), I/O, který prokažte nějakým veřejným Benchmarkem.	Ano
3	Velikost instalace agenta na koncovém zařízení do velikosti 100MB.	Ano
4	Předvídá pokročilé útoky kombinací statické a behaviorální inteligence.	Ano
5	Agent umožňuje sledovat a analyzovat behaviorální indikátory, které nejsou závislé na předchozí znalosti útoku a agent se rozhoduje, na základě těchto generických behaviorálních indikátorů zda zakročit.	Ano
6	Analýza podezřelých souborů je možná pomocí lokální analýzy (nevyžaduje zasílání neznámých souborů k analýze do sandboxu, připojení do cloudu, apod., bude tedy fungovat i offline)	Ano
7	Podpora zasílání bezpečnostních indicentů z centrálního serveru na SIEM.	Ano
8	Ochrana agenta proti snaze o deaktivaci nebo modifikaci procesů.	Ano
9	Ochrana úmyslného smazání stinových kopií operačního systému.	Ano
10	Plně šifrovaná a komprimovaná komunikace mezi agenty a centrálním serverem. Šifrování postavené na TLS.	Ano
11	Otevřené API s plnou dokumentací	Ano
12	Ochrana systému před poškozením nebo modifikací s možností vrácení systému do stavu před poškozením.	Ano
	Proaktivní bezpečnost	
13	Antivirový engine (signatury).	Ano
14	Využívání vícevrstvého přístupů k identifikaci neznámých hrozeb a) před exekucí (statická AI) - zkoumání souborů na podezřelé charakteristiky b) za běhu (behaviorální AI) - zkoumání chování běžících aplikací	Ano
15	Po zaznamenání hrozby nastává automatická reakce. Podezřelé procesy jsou ukončeny, podezřelé soubory přesunuty do karantény. V případě potřeby je možno zahájit automatické čištění nebo rollback systému.	Ano
16	Identifikace anti-detekčních mechanismů.	Ano
17	Behaviorální analýza síťové komunikace	Ano

18	Behaviorální analýza meziprocesové komunikace.	Ano
19	Behaviorální analýza souborové aktivity.	Ano
20	Behaviorální analýza operační paměti.	Ano
21	Behaviorální analýza systémové konfigurace.	Ano
22	Detekce útoků zaměřených na práci s pamětí (buffer, heap, stack under/overflow).	Ano
23	Využití Threat Intelligence zdrojů od alespoň 5 poskytovatelů.	Ano
24	Virtuální patching zero-day zranitelností.	Ano
	Náprava incidentů a forenzní analýza	
25	Izolace infikovaného koncového zařízení od sítě, ale zachováním spojení s centrálním serverem.	Ano
26	Analýza vektorů útoku v reálném čase ukazující příběhovou linii s plným záznamem všech souvisejících událostí, od práce se soubory, meziprocesorové komunikace, přes síťovou komunikaci až po využití exploitů.	Ano
27	Detekce laterálního pohybu, tedy pohybu na ostatní koncová zařízení.	Ano
28	Analýza aplikačního workflow souvisejícího s incidentem.	Ano
29	Schopnost automaticky vrátit provedené změny na koncové stanici (rollback systému).	Ano
30	Schopnost automaticky vrátit soubory do nezašifrované podoby.	Ano
31	Schopnost automaticky odstranit důsledky činností malware (smazat soubory, záznamy z registrů, ukončit procesy a zastavit služby).	Ano
32	Logování systémové a procesové aktivity pro další investigaci.	Ano
33	Logování síťových aktivit pro další investigaci.	Ano
	Správa a nasazení	
34	Vzdálená aktualizace agenta na koncovém zařízení.	Ano
35	Vzdálený restart či vypnutí koncového zařízeni.	Ano
36	Možnost zobrazit na obrazovce koncového zařízení zprávu od administrátora.	Ano
37	Možnost nasazení on-premise	Ano
38	Auditní záznam (activity logu).	Ano
39	Reporting přes email.	Ano
40	Možnost instalace agenta z MSI balíčku zahrnujícího i konfiguraci agenta.	Ano
41	dvou faktorová autentizace při přihlašování do management konzole	Ano
42	Ochrana agenta proti neautorizované odinstalaci.	Ano
	Ostatní	
43	Právní shoda PCI DSS, HIPPAA, GDPR, ISO27k	Ano