Akceptační testy

Jako podklad pro akceptaci budou provedeny následující testy:

Testování bude prováděno v místě plnění.

Test obecných požadavků na systém	Splňuje (ANO/NE)	Poznámka
systém zahrnuje všechny potřebné licence pro provoz Bezpečnostního monitoringu		
zpracovává a vyhodnocuje min. 10GB příchozích dat za den v jedné síťové infrastruktuře		
zpracovává a vyhodnocuje min. 5GB/den v jiné síťové infrastruktuře		
do systému je možné zasílat data z jakéhokoliv počtu typu zařízení s neomezeným počtem datových zdrojů		
systém pracuje ve virtualizačním prostředí RedHat Enterprise Virtualization		
systém umožňuje správu uživatelů a to pomocí systémů: lokání účty a LDAP (autorizace a autentizace)		
systém není licencován na počet uživatelů		
zadavatel se po převzetí díla (zaplacení) stane vlastníkem využitých licencí na neomezenou dobu		
při překročení objemu zpracovaných dat za den nedojde k zastavení zpracování nových příchozích dat		
systém garantuje zpracování všech událostí, při krátkodobém přetížení nedojde ke ztrátě logů a omezení funkcionality		
řešení bude dodáno jako samostatný virtuální stroj(e) nebo nástavba nad stávajícím řešení		
systém má prostředí v českém nebo anglickém jazyce		
zaznamenávat po nastavitelnou dobu vlastní auditní logy (viz § 21 vyhlášky č. 316/2014 Sb), které musí být chráněny proti modifikaci		
umožňuje v grafickém prostředí nastavovat/spravovat/vytvářet veškeré základní konfigurace definic zdrojů logů, definic korelačních pravidel, tvorbu reportů atd.; zpřesňující nastavení je možné provádět v textovém nebo jiném režimu		
Systém je podporován výrobcem po dobu požadované podpory		
požadované řešení není prototypem vyvinutým pro účel této veřejné zakázky		
systém je z aktuální produktové řady výrobce		

systém umožňuje rozšíření řešení až do min. množství zpracovaných dat 50GB/den v každé lokalitě		
Požadavky na test vyhodnocování bezpečnostních událostí		
systém umožňuje vyhledávání dle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech, v uložených log souborech a v auditních log souborech řešení		
systém rozlišuje zdroj log souborů		
log je dostupný v nezměněném tvaru, tak jak byl poslán ze zdrojového zařízení po dobu minimálně 90 dní		
systém vede evidenci a klasifikaci aktiv a identit, který je využíván pro výpočet kritičnosti událostí a incidentů		
systém umožňuje tagování pro jednotlivé události		
u aktiv a identit je vedena jejich váha a spojené riziko		
nad logy lze provádět parsování a extrakci polí		
systém je schopen nad logy provádět normalizaci, systém obsahuje datové struktury pro normalizované logy		
systém obsahuje minimálně struktury normalizovaných logů vyplývajících z § 21 vyhlášky č. 316/2014 Sb.		
uživatel může v grafickém rozhraní tvořit vlastní datové struktury normalizovaných logů, definovat jejich strukturu a určovat jaké typy logů budou normalizovány do takových tabulek		
příchozí logy lze normalizovat a ukládat v jedné nebo více normalizovaných datových strukturách		
při normalizaci lze provádět doplňování dat z dalších zdrojů. (např. doplnit jméno počítače za základě jeho IP adresy, doplnit lokalitu dle GEO informace, provést dotaz do LDAP apod.)		
korelace lze provádět nad normalizovanými logy, tak i nad logy v původním formátu		
systém umí automaticky stanovit závažnost událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací		
systém umožňuje tagování pro jednotlivé události		
umožňuje vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době apod.) nebo datových tocích (např. neobvyklé toky dat)		
systém umožňuje tagování pro jednotlivé události		

každý uživatel může definovat vlastní způsob extrakce polí a tímto nedojde k ovlivnění dalších uživatelů. Nová extrakce polí musí být aplikovatelná na již dříve uložená data stejně jako na data nově příchozí.		
definování / přidávání vlastních korelačních pravidel a log parserů formou průvodce (wizardu) přímo v GUI bez nutnosti spolupráce s dodavatelem nebo výrobcem		
je možno provést real-time korelaci a korelaci v časovém okně několika hodin mezi událostmi z různých zdrojů (libovolných a nezávislých zdrojů předávajících data do systému)		
je možno provádět korelaci událostí dávkově importovaných do systému tj. korelaci událostí, které nejsou zařazovány real-time, ale např. prostřednictvím importů logů		
systém obsahuje komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z oblastí - Útoky robotů, červů a virů (chyby antivirů), Monitorování databází (Chyby a varování, přístupy do DB, konfigurace), Neoprávněný přístup k aplikacím (ověřování uživatelů, změny administrace a konfigurace), Monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a změny konfigurace, odmítnutá připojení, úspěšné a chybné přihlašovací aktivity, varování systémů IPS/IDS a využívání šíře pásma)		
na události lze navázat automatické akce, spuštění externího skriptu		
systém umožňuje notifikaci přes email s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti zdroje nebo celkového vyhodnoceného rizika události		
systém podporuje napojení nezávislých zdrojů obohacujících informací, v poznámce uveďte, jaké zdroje systém nativně podporuje		
systém v rámci GUI podporuje tvorbu vlastních editovatelných dashboardů a vizuálních analýz		
systém podporuje pokročilý Alert Management (výpočet závažnosti score události se skládá z vícero vstupů a využívá klasicikaci aktiva a identity)		
systém podporuje Anotace/Poznámky pro detekované alerty		
systém obsahuje workflow pro podporu řešení detekovaných událostí a incidentů		
incidenty je možno přiřadit řesiteli		
je možno sledovat stav řešení incidentů		

je možno měnit důležitost incidentů k řešení		
k incidentu je možno přiřadit výsledky dalšího vyhledávání souvislostí		
workflow ke každému incidentu obsahuje časovou osu, kde je možno sledovat veškeré akce řešitelů		
Definované zdroje dat splňují požadavky § 21 vyhlášky č. 316/2014 Sb.		
Jsou implementovány všechny zadavatelem definované zdroje dat		
Požadavky na test reportingu		
řešení obsahuje předdefinované reporty, které musí být modifikovatelné		
reporty jsou poskytovány reporty i ve formě grafů a tabulek		
řešení umožňuje provést reporty ve formátech PDF, HTML a CSV (V poznámce uveďte, jaké formáty jsou podporovány)		
řešení poskytuje report o aktivitách vybraných uživatelů resp. skupiny uživatelů		
řešení poskytuje pro každého uživatele vlastní personalizovaný dashboard		
Drill-down analýza v GUI tj. od obecnějších informací vedou linky na konkrétnější informace a to s využitím minimálního počtů kroků		
řešení podporuje automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému		