

## Požadavky na ověření funkčnosti nabízeného vzorku plnění

V rámci ověření splnění technických požadavků nabízeného řešení nabídek z pohledu, zda nabídky dodavatelů splňují vybrané parametry funkčnosti dle požadavků zadavatele, může být účastník vyzván zadavatelem k prezentaci nabízeného řešení, v takovém případě bude účastník povinen prokázat, že nabízené řešení je funkční v rozsahu všech funkcionalit vymezených níže.

Bude-li prezentace požadována, zadavatel zašle dodavateli výzvu k prezentaci nabízeného řešení tak, aby mezi jejím doručením a termínem prezentace uplynuly alespoň 3 pracovní dny. Výzva bude zaslána na kontaktní údaje uvedené v nabídce dodavatele.

### Postup ověření řádné funkčnosti vzorku plnění:

1. Místem prezentace nabízeného řešení je: Národní bezpečnostní úřad, Na Popelce 2/16, Praha 5.
2. Zadavatel v rámci testování ověří, zda funkčnost účastníkem nabízeného řešení splňuje základní požadované parametry uvedené v bodě č. 5.
3. Zadavatel umožní v rámci testování využití svého přístupu do Internetu (min. 10 Mbitů obousměrně), a prostory pro přípravu testu ověření funkčnosti. Ostatní potřebný HW a SW si zajistí na své náklady dodavatel.
4. Každý požadavek uvedený v bodě č. 5 bude při prezentaci dodavatelem ověřován v dokumentaci předložené dle bodu 2.3 Zadávací dokumentace.
5. Předmětem ověření budou následující požadavky:

### Požadavky na vyhodnocování bezpečnostních událostí

	požadavky	Pro splnění zadaného požadavku
a)	systém umožňuje tagování (označování) jednotlivých logů a událostí dle libovolných kritérií	Logy a události musí být označeny daným tagem. Při splnění více podmínek může být log nebo událost označena vícero tagy najednou
b)	systém umožňuje vyhledávání log záznamů, událostí a incidentů dle zadané kombinace tagů a dalších podmínek (dle časových kritérií, typu zdroje, IP adresy, uživatele)	Do vyhledávacího pole musí být zadán název tagu (resp. názvy více tagů spojených logickými spojkami) a pak budou vyhledány všechny logy a události, které jsou označeny tímto tagem
c)	systém vede evidenci aktiv a identit a jejich klasifikaci, která je využívána pro výpočet kritičnosti událostí a incidentů. Evidenci je možno plnit ručně nebo z externích zdrojů	Systém musí vést tabulku aktiv a identit, kde je definováno riziko a další informace, např. název aktiva, IP adresa, umístění, kategorie, jméno uživatele apod. Tabulku je možné editovat ručně, nebo plnit automaticky z externích databází
d)	systém automaticky počítá míru rizika (risk score) pro jednotlivá aktiva a identity dle jejich klasifikace a reálně zjištěných událostí a incidentů	Musí existovat dashboard a report, kde je zobrazeno kumulované riziko pro jednotlivá aktiva a identity

Příloha č. 9 Zadávací dokumentace - Požadavky na ověření  
funkčnosti nabízeného vzorku plnění

e)	systém je schopen nad logy provádět normalizaci a datové obohacování. Normalizací se rozumí sjednocení formátu logů stejného typu z různých zdrojů. Log je extrahován a zaveden do příslušného jednotného schématu. Za normalizaci se nepovažuje prostá extrakce datových polí z logů.	Příchozí logy z různých typů zařízení musí být uloženy v normalizované podobě – ve stejném formátu – např. logy z Windows a Linuxu, které definují přihlašovaného uživatele k systému, obsahují shodné položky, normalizace převede datum do stejného formátu a sjednotí různé časové zóny, upraví jméno a příjmení do správného pořadí
f)	systém obsahuje jednotlivé, oddělené datové struktury pro normalizované logy, minimálně pro následující skupiny normalizovaných logů: síťový provoz, autentizace, řízení změn, kybernetické události a incidenty, malware, aktualizace, rizika, databáze	V datových strukturách musí být shromažďovány logy příslušných typů v normalizovaném formátu. Ve struktuře autentizace budou zapsány všechny logy, které obsahují informaci o autentizaci uživatele – z Windows, Linux, firewallu, routerů. Ve struktuře síťový provoz budou normalizovaně vedeny všechny relevantní informace k síťovému provozu (NetFlow, logy z Firewallu)
g)	uživatel může v grafickém rozhraní definovat vlastní datové struktury normalizovaných logů, upravovat jejich detailní strukturu a určovat jaké typy logů budou normalizovány do takových struktur	Musí být možné definovat název datové struktury, provést definici jednotlivých polí, způsob uložení informace do těchto polí a určit pravidlo, jaké logy zde budou normalizovány
h)	příchozí logy lze normalizovat a ukládat v jedné nebo více normalizovaných datových strukturách	Jeden a ten samý log se musí objevit po normalizaci ve vícero datových strukturách najednou
i)	při normalizaci lze provádět datové obohacování (Doplnit jméno počítače na základě jeho IP adresy, doplnit lokalitu dle GEO informace, provést dotaz do LDAP apod.)	V datových strukturách musí být možné definovat pole, která jsou plněna pomocí datového obohacování. Uživatelské jméno je možné dotazem do LDAP rozšířit o informaci o lokalitě, jméno a příjmení, IP adresu lze doplnit o GEO informaci.
j)	korelace lze provádět nad normalizovanými logy, tak i nad logy v původním formátu	Musí být možné provádět automatické korelace, s cílem identifikovat události a incidenty, nad vícero logy současně jak nad raw tak i normalizovanými logy v datových tabulkách. Přihlášení sledovaného uživatele (normalizovaný log) se automaticky koreluje s jeho přístupy přes firewall k webovým stránkám na blacklistu (log v původním formátu) – koreluje se přes IP adresu
k)	systém umí automaticky stanovit závažnost událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací	Systém musí počítat risk score dle zdroje a cíle události nebo incidentu a na základě toho je stanovena závažnost aktuálně detekované události

Příloha č. 9 Zadávací dokumentace - Požadavky na ověření  
funkčnosti nabízeného vzorku plnění

l)	systém umožňuje v grafickém prostředí nastavovat/spravovat/vytvářet veškeré základní konfigurace definic zdrojů logů, definic korelačních pravidel, tvorby reportů atd.; zpřesňující nastavení je možné provádět v textovém nebo jiném režimu,	Základní konfigurace definic zdrojů logů, definic korelačních pravidel, tvorby reportů atd. je prováděna v grafickém prostředí, zpřesňující nastavení je nastavováno v textovém nebo jiném režimu.
m)	definování / přidávání vlastních korelačních pravidel a log parserů formou průvodce (wizardu) přímo v GUI bez nutnosti spolupráce s dodavatelem nebo výrobcem	GUI musí obsahovat wizard kde si uživatel vybírá jednotlivé zdroje dat pro korelaci a systém mu automaticky nabízí vhodné způsoby korelace mezi nimi
n)	systém umožňuje notifikaci přes email s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti zdroje nebo celkového vyhodnoceného rizika události	Při notifikaci musí být možné stanovit minimální závažnost události pro notifikaci. Závažnost události je stanovena dle celkového kumulovaného rizika.
o)	systém podporuje pokročilý Alert Management (výpočet závažnosti – risk score události se skládá z vícera vstupů a využívá klasifikaci aktiva a identity)	Pro výpočet závažnosti události je využita informace o míře rizika, která je definována v rámci aktiv a identit
p)	systém obsahuje workflow pro podporu řešení detekovaných událostí a incidentů	Systém musí obsahovat trouble ticket management systém. Je možno definovat alespoň název ticketu, povolené stavy, přechody stavů, důležitost, notifikace a řešitele
q)	incidenty je možno přiřadit řešiteli	Incident je možno přiřadit konkrétnímu uživateli systému, přičemž systém musí vést evidenci takového kroku.
r)	je možno sledovat stav řešení incidentů	Každý incident má definován stav, nový, v řešení, analýza, vyřešeno, odmítnuto
s)	je možno měnit důležitost incidentů k řešení	Každý incident má stanovenou závažnost. Tuto mohou oprávnění uživatelé měnit v průběhu řešení tohoto incidentu
t)	k incidentu je možno přiřadit výsledky dalšího vyhledávání souvislostí	V rámci řešení incidentu je možno k tomuto incidentu přiřadit výsledek dodatečného vyhledávání souvislostí v tabulkové podobě, ve formě reportu a grafu.
u)	workflow ke každému incidentu obsahuje časovou osu, kde je možno sledovat veškeré akce řešitelů	Veškeré akce řešitele při řešení incidentu jsou viditelné v časové ose. Tímto je možné sledovat průběh analýzy incidentu pro budoucí optimalizaci řešení.

Dodavatel musí být schopen poskytnout zadavateli záznam (např. formou PrtScr) o výsledku testování každé funkcionality/požadavku dle bodu 5 shora. Pokud dodavatel nebude schopen při prezentaci demonstrovat požadovanou funkčnost nabízeného řešení dle požadavků zadavatele, nesplňuje takové řešení požadavky zadavatele dle Zadávací

Příloha č. 9 Zadávací dokumentace - Požadavky na ověření  
funkčnosti nabízeného vzorku plnění

dokumentace.