Parameter	Minimálne Požadované vlastnosti	Splnenie požadovaných vlastností uchádzačom (uchádzač uvedie konkrétne parametre ponukaného riešenia)
Názov	**SIEM (Security Information and Event Management)**	**Výrobca: Cisco** **Model: Splunk Enterprise - Term License with Standard Success Plan - SE-T-LIC-ST** **Splunk Enterprise Security - Term License with Standard Success Plan - ES-T-LIC-ST**
Poradové číslo	**1**	**1**
Počet	**1**	**1**
Všeobecné požiadavky	Systém musí podporovať konfiguráciu s vysokou dostupnosťou, aby sa nestratili zhromaždené log záznamy v prípade zlyhania niektorej súčasti. Riešenie s vysokou dostupnosťou musí byť k dispozícii kedykoľvek v ďalších fázach projektu počas implementácie aj bez potreby preinštalovať pôvodný systém a migrovať údaje.	Systém podporuje konfiguráciu s vysokou dostupnosťou, aby sa nestratili zhromaždené log záznamy v prípade zlyhania niektorej súčasti. Riešenie s vysokou dostupnosťou je k dispozícii kedykoľvek v ďalších fázach projektu počas implementácie aj bez potreby preinštalovať pôvodný systém a migrovať údaje. Pre viac podrobností sa prosím obráťte na náš dokument o overených architektúrach splunk: https://docs.splunk.com/Documentation/SVA/current/Architectures/AboutApplied
	Všetky požadované funkcie sú spravované a používané prostredníctvom jednej spoločnej riadiacej konzoly, ktorá je prístupná prostredníctvom webového rozhrania s využitím štandardného prehliadača. Všetky používateľské nastavenia a vlastná práca so systémom sa vykonáva na jednom mieste z jednej spoločnej konzoly bez ohľadu na modul (správa protokolov, SIEM, analýza siete atď.).	Všetky požadované funkcie sú spravované a používané prostredníctvom jednej spoločnej riadiacej konzoly (Splunk web UI), ktorá je prístupná prostredníctvom webového rozhrania s využitím štandardného prehliadača. Všetky používateľské nastavenia a vlastná práca so systémom sa vykonáva na jednom mieste z jednej spoločnej konzoly bez ohľadu na modul (správa protokolov, SIEM, analýza siete atď.). WEB UI zahŕňa nielen správu protokolov, SIEM, rôzne panely zobrazenia týkajúce sa údajov o sieti, identitných údajov, cloudovej bezpečnosti a pod., ale aj integráciu SOAR, kde môžu bezpečnostní analytici využívať Splunk SOAR priamo z rozhrania SIEM (vyšetrenie incidentov, obohatenie a reakcia prostredníctvom Splunk SOAR, všetko z konzoly SIEM).
	Centrálna správa Siem musí podporovať GUI (Grafické používateľské rozhranie).	Centrálna správa Siem musí podporovať GUI (Grafické používateľské rozhranie). Splunk ponúka webové rozhranie Splunk Web pre správu platformy.
	Všetky konfigurácie, definície zdrojov protokolov, definícia korelačných pravidiel, podávanie správ atď. musí prebiehať z grafického rozhrania SIEM bez toho, aby bolo potrebné zasahovať do programového kódu.	Všetky konfigurácie, definície zdrojov protokolov, definícia korelačných pravidiel, podávanie správ atď. prebieha z grafického rozhrania SIEM bez toho, aby bolo potrebné zasahovať do programového kódu. Grafické používateľské rozhranie Splunk (GUI) sa dá použiť na konfiguráciu, definovanie zdrojov protokolov, definovanie korelačných pravidiel, tvorbu reportov a ďalšie.
	Správa používateľov SIEM musí podporovať integráciu s Microsoft Active Directory (AD) / Privileged Access Management (PAM)	Správa používateľov SIEM podporuje integráciu s Microsoft Active Directory (AD) / Privileged Access Management (PAM), konkrétne Platforma Splunk sa dokáže integrovať s AL/LDAP a SAML pre overovanie používateľa. Viac podrobností nájdete v dokumentácii nižšie: https://docs.splunk.com/Documentation/Splunk/9.2.1/Security/SetupuserauthenticationwithLDAP
	SIEM musí tiež umožniť prihlasovanie pomocou lokálnych účtov (v prípade nedostupnosti AD).	SIEM umožňuje prihlasovanie pomocou lokálnych účtov (v prípade nedostupnosti AD), konkrétne Splunk ponúka natívny mechanizmus overovania ako štandardný spôsob overovania na platforme Splunk. Je štandardnou súčasťou každej inštalácie Splunk Enterprise. https://docs.splunk.com/Documentation/Splunk/latest/Security/Setupbuilt-inauthentication
	Prístup používateľov musí byť založený na definovaných samostatných rolách s možnosťou podrobného prideľovania práv v rámci roly podľa zdrojov loga, skupiny zariadení, jednotlivých serverov, typu logu atď.	Splunk ponúka rozsiahle možnosti riadenia prístupu na základe rolí (RBAC) na určovanie práv každého používateľa/roly na platforme. Administrátori môžu rozhodnúť o dátach a funkciách, ku ktorým má každý používateľ/rola prístup v rámci platformy Splunk. Pri integrácii s AD/LDAP je tiež možné mapovať vaše AD/LDAP role na role Splunk pre jednoduchšiu správu. Pre viac informácií, prosím, pozrite si dokumentáciu nižšie: https://docs.splunk.com/Documentation/Splunk/9.2.1/Security/MapLDAPgroupstoSplunkroles https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/setpermissionsforobjects/
	Systém SIEM musí vyhľadávať podľa kľúčových slov (reťazcov) v názvoch zdrojov, korelačných pravidlách v uložených logoch a v auditných logoch systému.	Splunk podporuje voľné vyhľadávanie kľúčových slov/textové vyhľadávanie, ktoré umožňuje vyhľadávať na základe kľúčových slov/reťazcov bez ohľadu na zdroj informácií.
	Systém SIEM zaznamenáva svoje vlastné auditné logy počas nastaviteľného časového obdobia.	Po zapnutí auditu platforma Splunk odosiela špecifické udalosti do auditorského indexu (index=_audit). Interakcie s platformou, ako sú vyhľadávania, prihlásenia a odhlásenia, kontroly oprávnení a zmeny konfigurácie, generujú auditorské udalosti. Auditorský protokol obsahuje nasledujúce informácie: Časové razítko: dátum a čas udalosti. Informácie o používateľovi: používateľ, ktorý udalosť vygeneroval. Ak udalosť neobsahuje informácie o používateľovi, platforma Splunk nastaví používateľa na toho, kto je momentálne prihlásený. Dodatočné informácie: dostupné podrobnosti o udalosti – aký súbor, úspech/zamietnutie, atď. Nasledujúce aktivity generujú auditorské udalosti na platforme Splunk: Všetky súbory v konfiguračnom adresári Splunk Enterprise $SPLUNK_HOME/etc/* Súbor je monitorovaný na pridanie/zmenu/odstránenie pomocou monitora zmien súborového systému. Štart a zastavenie inštancie. Používatelia sa prihlasujú a odhlasujú z platformy. Pridávanie a odstraňovanie používateľov. Zmena informácií o používateľovi (heslo, rola, atď.). Spustenie ľubovoľnej funkcie na platforme – Funkcie sú uvedené v súbore authorize.conf Pre viac podrobností, prosím, pozrite si dokumentáciu nižšie: https://docs.splunk.com/Documentation/Splunk/9.2.1/Security/AuditSplunkactivity
	Systém SIEM musí byť schopný využívať detegované anomálie a informácie zo siete pre koreláciu udalostí do jednotných incidentov pre spresnenie kontextu a zníženie false-positives nálezov.	Presne to ponúka Splunk metodika založená na riadení rizika (Risk Based Alerting - RBA), ktorá sa vyvinula do nových detekcií založených na zisteniach (Finding-Based detections). Koreluje rôzne anomálie týkajúce sa tej istej entity do jedného upozornenia, ktoré obsahuje všetky prepojené anomálie/incidenty. Táto metodika je veľmi užitočná na zníženie falošne pozitívnych výsledkov, pretože dokáže zoskupiť viacero falošne pozitívnych výsledkov do jedného upozornenia. To umožňuje znížiť počet falošne pozitívnych výsledkov, celkový počet upozornení a zároveň zvýšiť podiel skutočne pozitívnych výsledkov, pretože RBA dokáže detekovať aj „pomalé a tiché" útoky počas dlhšieho časového obdobia. Viac informácií o našej metodike RBA a jej novom „vývoji", detekciách založených na zisteniach, nájdete nižšie: https://docs.splunk.com/Documentation/ES/8.0.2/User/AnalyzeInvestigationEvents https://docs.splunk.com/Documentation/ES/8.0.2/Admin/FindingBasedDetections
	Jednoduché pripojenie alebo natívne rozšírenie s funkčnosťou systému správy rizík (analýza zraniteľnosti, stanovenie priorít, topológia siete).	SIEM systém Splunk ponúka natívne funkcie riadenia rizík prostredníctvom nášho rámca pre riadenie rizík a rámcov pre aktíva a identity, čo umožňuje analytikom lepšie prioritizovať hrozby. Pre viac podrobností, prosím, pozrite si našu dokumentáciu nižšie: https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/assetandidentityframework/
	Schopnosť spracovať všetky typy logov, bez ohľadu na štruktúru a zdroj	Áno. Splunk dokáže prijať akýkoľvek log čitateľný človekom bez ohľadu na zdroj a štruktúru.
Požiadavky na výkon a škálovateľnosť	Systém SIEM musí mať jasne uvedenú licenčnú politiku a to vrátane uvedenia funkcionalít, ktoré nie sú súčasťou požadovanej licencie, a to preukázaním produktového katalógu.	Áno. Splunk a SIEM riešenie (Splunk Enterprise Security) sú licencované na základe celkovej veľkosti prijatých dát (v GB) za deň. Neexistujú žiadne „skryté poplatky" ani žiadne extra funkcie, ktoré by neboli zahrnuté v licencii Splunk a Splunk ES. Po zakúpení produktu sú dostupné všetky funkcie. Viac podrobností o licencovaní Splunk nájdete tu: https://docs.splunk.com/Documentation/Splunk/9.4.0/Admin/TypesofSplunklicenses
	Systém SIEM musí byť nainštalovaný lokálne a ľahko rozšíriteľný z hľadiska funkčnosti a výkonu bez toho, aby bola ohrozená investícia, ktorá sa už v minulosti urobila (starý komponent (HW a SW) sa musí ďalej používať, nie vyraďovať).	Áno. Platforma Splunk sa dá škálovať vertikálne aj horizontálne, čo umožňuje škálovanie bez ohrozenia predošlých investícií. Pre viac podrobností sa prosím, obráťte na náš dokument o overených architektúrach Splunk: https://docs.splunk.com/Documentation/SVA/current/Architectures/AboutApplied
	Systém SIEM musí byť schopný spracovať a uchovať logy z nasledovných zdrojov (pri nastavení podľa odporúčaní výrobcu SIEM): - 13 tisíc užívateľov Microsoft Office 365 - 4 tisíc užívateľov Microsoft Teams a Microsoft Sharepoint - 16 tisíc pracovných staníc - 10 Active Directory serverov - 4 Exchange servery - 250 Windows Server a 250 Linux serverov - 16 virtualizačných / HCI serverov - 200 wifi Access Point - 2 wifi Controller - 300 sieťových prepínačov - 100 sieťových smerovačov - 20 firewallov - 3 proxy servery slúžiace pre 13 tisíc užívateľov a 500 serverov - 2 Network Access Control zariadenia - 4 DNS servery - 20 DHCP serverov - 4 loadbalancing zariadenia - 40 databázových inštancií - 60 webových serverov - 40 aplikačných serverov - 1 systém pre správu zraniteľností pre 16800 IP zariadení - 2 zariadenia pre behaviorálnu analýzu siete - 1 EDR systém pre 16800 zariadení Minimálne požiadavky spracovať a uchovať sú: 30 000 EPS a 400GB za deň a 250 000 fpm (dátových tokov/minúta). Požadovaný výkon (EPS, spracovaný objem dát alebo počet flow) musí určiť uchádzač štandardným nástrojom na kvalifikovaný odhad potrebného výkonu nástrojmi výrobcu SIEM a uviesť jeho výstup do ponuky ako samostatnú záložku tejto prílohy.	Áno. Splunk dokáže prijať až niekoľko petabajtov dát denne, čo výrazne prekračuje požiadavku ministerstva 400 GB/deň a 250 000 fpm (dátových tokov/minúta). Podporované zdroje zahŕňajú, ale nie sú obmedzené na: koncové body, MS Office, MS Cloud, iných poskytovateľov cloudu, MS AD, servery Windows a Linux, sieťové zariadenia (routery, switche, firewally, proxy servery, prístupové body, atď.) a ďalšie. Pre úplný zoznam dostupných integrácií, prosím, pozrite si našu Splunkbase nižšie: https://splunkbase.splunk.com/apps

	SIEM nesmie technicky obmedziť počet udalostí (napríklad v prípade prekročenia licencie alebo výkonu zakúpeného riešenia), tak aby došlo k strate udalostí.	Áno. Splunk vždy uprednostní prijímanie dát a nebude dáta vyhadzovať, ani v prípade prekročenia licenčného limitu. Upozorňujeme však na možný vplyv prekročenia limitu na výkon platformy; pokiaľ sú k dispozícii dostatočné hardvérové zdroje na prijímanie prichádzajúcich dát, platforma bude túto úlohu vždy uprednostňovať.
	Systém SIEM musí podporovať automatickú archiváciu logovacích záznamov na externé úložisko podľa vybraných kritérií (podľa veku, typu loga, zdroja atď.)	Áno. Používatelia sa môžu rozhodnúť, ako a kedy archivovať dáta na základe kritérií, ako je vek, veľkosť, typ/zdroj logu atď. Viac informácií o tom, ako funguje archivovanie, nájdete v dokumentácii nižšie: https://docs.splunk.com/Documentation/Splunk/9.2.1/Indexer/Automatearchiving
	Systém SIEM musí podporovať simultánnu prácu najmenej 3 používateľov s aktívnym prístupom (plná funkčnosť) a 3 pracovníkov s pasívnym prístupom (reporty, vlastné dasboary, ale bez administrátorských práv na zmenu konektorov a systémového nastavenia).	Áno. Splunk Enterprise podporuje maximálne 2000 súbežných používateľov. Keďže riešenie SIEM nie je cenené na základe počtu používateľov, zákazníci môžu poskytnúť ľubovoľný prístup/funkcie podľa potreby; nebude sa účtovať viac za určitých používateľov a menej za iných. https://docs.splunk.com/Documentation/Splunk/9.2.1/Capacity/Service
Požiadavky na zber údajov	Licencia musí obsahovať možnosť zbierať všetky typy výrobcom podporovaných zdrojov podľa dokumentácie výrobcu.	Áno. Splunk dokáže prijať akýkoľvek log čitateľný človekom, bez ohľadu na zdroj. Podporované zdroje zahŕňajú, ale nie sú obmedzené na: koncové body, MS Office, MS Cloud, iných poskytovateľov cloudu, MS AD, servery Windows a Linux, sieťové zariadenia (routery, switche, firewally, proxy servery, prístupové body atď.) a ďalšie. Pre úplný zoznam dostupných integrácií, prosím, navštívte našu Splunkbase: https://splunkbase.splunk.com/apps
	Musí podporovať zber logov bez zasahovania do systémov z ktorých sa logy berú (bez agentový zber).	Áno. Splunk podporuje bezagentné zhromažďovanie dát prostriedkami ako WMI, syslog, API, Splunk HEC, atď. Proces získavania dát (GDI) vo Splunku je detailne zdokumentovaný: https://docs.splunk.com/Documentation/Splunk/latest/Data/Getstartedwithgettingdatain
	Musí podporovať zber udalostí zo sieťových zariadení a ich parsovanie s cieľom identifikovať útoky na vrstvu L3 a L2	Áno. Splunk dokáže prijať sieťové dáta a analyzovať informácie na vrstvách L2 a L3.
	Musí podporovať načítanie súborov logov, bez ohľadov na to, či majú alebo nemajú definovanú štruktúru a význam údajov (structured, semi structored unstructured)	Áno. Splunk dokáže prijať akýkoľvek log čitateľný človekom, bez ohľadu na zdroj a formát. Ponúkame viac ako 2000 hotových integrácií dostupných na Splunkbase: https://splunkbase.splunk.com/apps
	Musí podporovať získavanie protokolov z databázy (najmä MS SQL, Oracle a PostgeSQL), kde tieto protokoly budú mať definovanú štruktúru a význam údajov.	Áno. Splunk DB Connect je univerzálne rozšírenie pre databázy SQL pre Splunk, ktoré umožňuje jednoduchú integráciu informácií z databáz s dotazovaním a reportovaním vo Splunku. Splunk DB Connect podporuje DB2/Linux, Informix, MemSQL, MySQL, AWS Aurora, Microsoft SQL Server, Oracle, PostgreSQL, AWS RedShift, SAP SQL Anywhere, Sybase ASE, Sybase IQ, Teradata, InfluxDB a MongoDB Atlas & Standalone. https://splunkbase.splunk.com/app/2686
	Musí umožňovať načítanie a spracovanie rôznych typov logov, a to aj z vlastných aplikácií. Táto možnosť musí byť dostupná prostredníctvom používateľského rozhrania bez potreby súčinnosti výrobcu alebo dodávateľa riešenia a bez toho, aby pracovník musel poznať programovacie jazyky.	Áno. Splunk dokáže prijať akýkoľvek log čitateľný človekom, bez ohľadu na zdroj a formát. Ponúka viac ako 2000 hotových integrácií na Splunkbase a ak niektorá integrácia nie je dostupná, ponúkame nástroj Splunk Add-on Builder pre jednoduché vytváranie vlastných analyzátorov priamo cez rozhranie Splunk používateľom, bez nutnosti znalosti programovacích jazykov. Splunkbase: https://splunkbase.splunk.com/apps Splunk Add-on Builder: https://splunkbase.splunk.com/app/2962
	Musí umožniť centralizáciu jednotlivých zdrojov logov do jedného dátového kanála, ktorý je potom integrovaný do centrálneho prvku (pripojenie zdrojov logov zo vzdialených lokalít len s jedným prestupom cez FW).	Áno. Presne to je úloha Splunk Heavy Forwarder (HF). Môže slúžiť ako jediný bod zberu všetkých vašich dát a potom len HF komunikuje s platformou Splunk pre prenos dát.

Požiadavky na spracovanie udalostí	Systém SIEM musí umožňovať používanie regulárnych výrazov pre parsovanie logovacích údajov	Áno. Splunk podporuje používanie regulárnych výrazov (REGEX) pre analýzu logov a vyhľadávanie. Upozorňujeme, že hoci sa REGEX používa pre analýzu logov, tento proces má byť pre koncového používateľa transparentný, pretože Splunk vykoná analýzu za vás. Môžete však pridať ďalšiu logiku analýzy pomocou REGEX priamo cez rozhranie Splunk. Príkladom je náš nástroj Field Extractor, zdokumentovaný nižšie: https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/ExtractfieldsinteractivelywithIFX
	Systém SIEM musí umožňovať normalizáciu bezpečnostných udalostí v systéme SIEM do jednotného formátu (centrálne logy musia mať rovnaký formát zo všetkých zdrojov) a doplnenie o ďalšie detailné informácie (napr. Doplnenie používateľského mena na základe používateľského účtu atď.).	Áno. Splunk normalizuje dáta pomocou Splunk Common Information Model (CIM) a môže obohatiť/poskytnúť kontext pomocou rámca Asset&Identity. https://docs.splunk.com/Documentation/CIM/5.3.2/User/Overview
	Systém SIEM musí umožňovať kategorizáciu logov poskytovanú univerzálnou taxonómiou nezávislou od výrobcu zdroja udalostí, aby bolo možné udalosti homogénne vyhľadávať, reportovať alebo porovnávať udalosti z rôznych zariadení bez toho, aby bolo potrebné poznať konkrétny log	Áno. Splunk normalizuje dáta pomocou Splunk Common Information Model (CIM), univerzálnej taxonómie nezávislej od výrobcu zdroja udalosti, čo umožňuje homogénne vyhľadávanie, reportovanie alebo porovnávanie udalostí z rôznych zariadení bez potreby znalosti špecifického logu. https://docs.splunk.com/Documentation/CIM/5.3.2/User/Overview
	Systém SIEM musí umožňovať zobrazenie a zmenu nasadených pravidiel korelácie vrátane pravidiel dodaných výrobcom.	Áno. Všetky detekcie vo Splunku, vrátane tých, ktoré poskytujeme my, sa dajú zobraziť a upraviť podľa potreby.
	Systém SIEM musí umožňovať definovanie/pridávanie vlastných korelačných pravidiel a log parserov bez potreby spolupráce s dodávateľom alebo výrobcom, napr. Pomocou wizardu alebo regulárnych výrazov	Áno. Používatelia Splunku môžu jednoducho vytvárať nové detekcie pomocou nášho rozhrania bez potreby externej pomoci, ako je zdokumentované nižšie: https://docs.splunk.com/Documentation/ES/8.0.2/Admin/ConfigureFindingsBasedDetections Pokiaľ ide o nové pravidlá analýzy, ponúkame nástroj Splunk Add-on Builder pre jednoduché vytváranie nových analyzátorov dát (na báze rozhrania; podporuje používanie REGEX), ak nie je dostupný hotový analyzátor. Ako je uvedené vyššie, ponúkame aj zabudovanú funkciu extraktora polí na báze rozhrania, ktorá môže použiť REGEX na analýzu vašich logov. Splunk add-on builder: https://splunkbase.splunk.com/app/2962 Splunk field extractor: https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/ExtractfieldsinteractivelywithIFX
	Systém SIEM musí umožňovať Real-time koreláciu a koreláciu v časovom okne min..4 hodín medzi udalosťami z rôznych zdrojov (ľubovoľných a nezávislých zdrojov prenášajúcich údaje do systému)	Áno. Splunk podporuje vyhľadávanie a koreláciu v reálnom čase aj historické vyhľadávanie/koreláciu. Dáta z nezávislých zdrojov prenášané do systému sa dajú vyhľadávať/korelovať bez ohľadu na časový rámec (pokiaľ sú dáta prítomné na platforme Splunk).
	Systém SIEM musí umožňovať automatické určenie závažnosti udalostí, napr. na základe predošlej činnosti zdroja/cieľa alebo iných dostupných informácií.	Áno. Splunk dokáže nastaviť naliehavosť incidentu na základe napadnutého aktíva. Môžeme tiež zobraziť skóre „rizika“ napadnutého aktíva na základe iných incidentov, ktoré sa na ňom vyskytli. To znamená napríklad, že útok proti generálnemu riaditeľovi bude mať oveľa vyššiu naliehavosť/skóre rizika ako ten istý útok proti stážistovi.
	Systém SIEM musí umožňovať vyhľadávanie anomálií v udalostiach (napr. nárast počtu neúspešných pokusov o prihlásenie v určitom čase, neúspešné pokusy o prihlásenie v mimopracovnej dobe, atď.) alebo dátových tokov (napr. nezvyčajné toky údajov)	Áno. Splunk dokáže vytvoriť základnú líniu správania používateľa a potom upozorniť na zistené anomálie; to zahŕňa, ale nie je obmedzené na: zvýšenie počtu neúspešných pokusov o prihlásenie v určitom čase, neúspešné pokusy o prihlásenie mimo pracovnej doby, dátové toky (napr. nezvyčajné dátové toky) atď
	Systém SIEM musí umožňovať agregáciu udalostí (logy, flow) do jedného identifikovaného incidentu, ak udalosti súvisia s tým istým incidentom	Áno. Presne to ponúka metodika založená na riadení rizika (RBA) alebo novovytvorené detekcie založené na zisteniach, ktoré korelujú rôzne anomálie týkajúce sa tej istej entity do jedného upozornenia obsahujúceho všetky prepojené anomálie/incidenty. Viac informácií o našej metodike RBA a jej novom „vývoji“, detekciách založených na zisteniach, nájdete nižšie: https://docs.splunk.com/Documentation/ES/8.0.2/User/AnalyzeInvestigationEvents https://docs.splunk.com/Documentation/ES/8.0.2/Admin/FindingBasedDetections
	Na akúkoľvek udalosť musí byť možné nadviazať automaticky	Na akúkoľvek udalosť je možné nadviazať automaticky. Všetky požiadavky uvedené nižšie sú podporované.
	- notifikáciu prostredníctvom e-mailu s možnosťou definovať pravidlá zasielanie na rôzne adresy podľa kritickosti, zdroja atď.	Možné pomocou akcie "Odoslať email" https://docs.splunk.com/Documentation/Splunk/9.4.0/Alert/Emailnotification
	- spustenie externého skriptu	Možné pomocou Adaptívnej odpovede alebo vlastnej akcie upozornenia – vytvoríte skript a Splunk ho môže spustiť ako súčasť automatickej odpovede na incident. https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/adaptiveresponseframework/ https://dev.splunk.com/enterprise/docs/devtools/customalertactions/
	Musí obsahovať komplexná sadu funkcionalít a prednastavených pravidelne aktualizovaných korelačných pravidiel (min. 1000), ktoré riešia hrozby a bezpečnostné riziká, ako aj bezpečnostné problémy z rôznych oblastí:	Áno – všetky požiadavky uvedené nižšie sú podporované. Obsahuje komplexná sadu funkcionalít a prednastavených pravidelne aktualizovaných korelačných pravidiel (min. 1000), ktoré riešia hrozby a bezpečnostné riziká, ako aj bezpečnostné problémy z rôznych oblastí:
	- Útoky robotov, červov a vírusov (chyby antivírusové)	Poskytuje hotové detekcie pre tento prípad použitia. Zoznam viac ako 1800 hotových detekcií pre zákazníkov Splunk nájdete nižšie: https://research.splunk.com/detections/ (Táto odpoveď sa opakuje pre niekoľko kategórií hrozieb)
	- Monitorovanie databáz (chyby a varovania, prístup do DB, konfigurácia)	Poskytuje hotové detekcie pre tento prípad použitia. Zoznam viac ako 1800 hotových detekcií pre zákazníkov Splunk nájdete nižšie: https://research.splunk.com/detections/ (Táto odpoveď sa opakuje pre niekoľko kategórií hrozieb)
	- Neoprávnený prístup k aplikáciám (overovanie používateľov, zmeny administrácie a konfigurácie)	Poskytuje hotové detekcie pre tento prípad použitia. Zoznam viac ako 1800 hotových detekcií pre zákazníkov Splunk nájdete nižšie: https://research.splunk.com/detections/ (Táto odpoveď sa opakuje pre niekoľko kategórií hrozieb)
	- Chyby a zmeny v sieťach (chyby a stavy sieťových zariadení)	Poskytuje hotové detekcie pre tento prípad použitia. Zoznam viac ako 1800 hotových detekcií pre zákazníkov Splunk nájdete nižšie: https://research.splunk.com/detections/ (Táto odpoveď sa opakuje pre niekoľko kategórií hrozieb)
	- Monitorovanie serverov a desktopov (administrácia privilegovaných používateľov, prístupy a zmeny konfigurácie, odmietnuté pripojenia, úspešné a chybné prihlasovacie aktivity, upozornenia systémov IPS/IDS a využitie šírky pásma)	Poskytuje hotové detekcie pre tento prípad použitia. Zoznam viac ako 1800 hotových detekcií pre zákazníkov Splunk nájdete nižšie: https://research.splunk.com/detections/ (Táto odpoveď sa opakuje pre niekoľko kategórií hrozieb)
	- Útoky VPN (chyby pri overovaní, zmeny konfigurácie, aktivita pripojovania)	Poskytuje hotové detekcie pre tento prípad použitia. Zoznam viac ako 1800 hotových detekcií pre zákazníkov Splunk nájdete nižšie: https://research.splunk.com/detections/ (Táto odpoveď sa opakuje pre niekoľko kategórií hrozieb)
	- Zabratie šírky pásma a porušenie platných pravidiel (úspešné a chybné prihlásenia do systému, zmeny hesla, zmeny konfigurácie	Poskytuje hotové detekcie pre tento prípad použitia. Zoznam viac ako 1800 hotových detekcií pre zákazníkov Splunk nájdete nižšie: https://research.splunk.com/detections/ (Táto odpoveď sa opakuje pre niekoľko kategórií hrozieb)
Požiadavky na archiváciu a ukladanie	Systém SIEM musí umožňovať pripojenie k vyhradenému externému úložisku bezpečnostných udalostí	Áno. Splunk sa dokáže integrovať s externým systémom tretích strán pomocou API.
	Systém SIEM musí umožňovať interne ukladať údaje bez straty informácií, RAW logy (bez filtrácie, normalizácie, redukcie) a aj normalizovať ukladané údaje	Áno. Splunk nemení surové (RAW) logy – vaše surové dáta sa ukladajú bez akýchkoľvek zmien/strát informácií. Schému používame pri vyhľadávaní pre normalizáciu.
	Systém SIEM musí umožňovať interne uchovávať normalizované log záznamy	Áno. Hoci Splunk používa normalizáciu pri vyhľadávaní (čo znamená, že ukladáme surové logy tak, ako prichádzajú, bez akýchkoľvek zmien), môžeme tiež interným spôsobom ukladať normalizovanú „verziu“ pomocou toho, čo nazývame Data Model Acceleration – spôsob, ako ukladať normalizované, štruktúrované dáta spôsobom, ktorý umožňuje Splunku vykonávať výkonné vyhľadávania. https://docs.splunk.com/Documentation/Splunk/9.4.0/Knowledge/Acceleratedatamodels
	Systém SIEM musí umožňovať ukladanie údajov v komprimovaných formách pre úsporu diskovej kapacity	Áno. Ako pravidlo môžeme predpokladať 50% kompresiu (surové komprimované dáta + tsidx dáta). https://docs.splunk.com/Documentation/Splunk/9.2.1/Capacity/Estimateyourstoragerequirements
	SIEM musí byť schopný automaticky archivovať logy podľa požiadaviek DR a HA capabilities	Áno. Splunk umožňuje zákazníkom nastaviť si vlastné pravidlá pre archivovanie logov podľa veľkosti logov, veku, typu/zdroja atď. prostredníctvom indexov. Splunk podporuje funkcie obnovy po havárii s rozsiahlym zoskupeným nasadením na viacerých miestach; zákazníci môžu tiež pravidelne zálohovať svoje dáta (podporované sú prírastkové a úplné zálohy). V susednom stĺpci poskytujeme dokumentáciu o možnostiach nasadenia na viacerých miestach a o možnostiach zálohovania. https://docs.splunk.com/Documentation/SVA/current/Architectures/M2M12 https://docs.splunk.com/Documentation/Splunk/9.2.1/Admin/Backupconfigurations https://docs.splunk.com/Documentation/Splunk/9.2.1/Indexer/Backupindexeddata
	Systém musí umožniť jednoduché obnovenie historických údajov z archívov pre spätnú analýzu	Áno. Splunk umožňuje zákazníkom jednoducho obnoviť archivované dáta procesom, ktorý nazývame „rozmrazovanie“. https://docs.splunk.com/Documentation/Splunk/9.4.0/Indexer/Restorearchiveddata
	Systém musí umožniť rýchle obnovenie uložených logov pre prípad obnovy systému po prípadnej havárii	Áno. Splunk podporuje obnovenie po havárii prostredníctvom nasadenia na viacerých miestach a záloh archivovaných dát. Splunk umožňuje zákazníkom jednoducho obnoviť archivované dáta procesom, ktorý nazývame „rozmrazovanie“. https://docs.splunk.com/Documentation/SVA/current/Architectures/M2M12 https://docs.splunk.com/Documentation/Splunk/9.2.1/Admin/Backupconfigurations https://docs.splunk.com/Documentation/Splunk/9.2.1/Indexer/Backupindexeddata https://docs.splunk.com/Documentation/Splunk/9.2.1/Indexer/Restorearchiveddata
	Systém musí poskytnúť mechanizmus detekcie neoprávnených zmien údajov (zmena logov pred importom musí byť rozpoznaná)	Nie je možné upravovať dáta, ktoré už boli prijaté do platformy Splunk.
	Systém SIEM musí umožňovať zabezpečenie integrity archivačných súborov (napr. digitálny podpis, hash, šifrovaním, atď.)	Áno. Kontrola integrity dát Splunk Enterprise vám pomôže overiť integritu dát, ktoré indexuje. Keď povolíte kontrolu integrity dát pre index, Splunk Enterprise vypočíta hashe pre každú časť dát pomocou algoritmu SHA-256. Potom uloží tieto hashe, aby ste neskôr mohli overiť integritu vašich dát. https://docs.splunk.com/Documentation/Splunk/9.2.1/Security/Dataintegritycontrol
	Systém SIEM musí umožňovať filtrovanie udalostí pred archiváciou	Áno. Filtrovanie sa môže uskutočniť na úrovni agenta (bližšie k zdroju) alebo na vrstve indexovania, tesne pred prijatím dát. V každom prípade, filtrované dáta sa nepočítajú do vašej licencie na prijímanie dát. Veľmi jednoduchý a výkonný spôsob filtrovania dát pred indexovaním je použitie našej funkcie Ingest Actions; Ingest actions je funkcia pre smerovanie, filtrovanie a maskovanie dát počas ich prenosu do vašich indexérov. Každá transformácia dát je vyjadrená ako pravidlo. Môžete použiť viacero pravidiel na dátový tok a uložiť kombinované pravidlá ako sadu pravidiel. https://docs.splunk.com/Documentation/Splunk/9.4.0/Data/DataIngest

	Systém SIEM musí podporovať pravidelné automatické presuny údajov z interného do externého úložiska alebo archívu podľa definovaných pravidiel	Áno. Používatelia sa môžu rozhodnúť, ako a kedy archivovať dáta na základe kritérií, ako je vek, veľkosť, typ/zdroj logu atď. Dáta sa môžu archivovať na externé úložisko. https://docs.splunk.com/Documentation/Splunk/9.2.1/Indexer/Automatearchiving

Požiadavkyna reporting a interpretáciu údajov	Preddefinované a modifikovateľné reporty systému SIEM	Áno. Splunk Enterprise Security (ES), ponúka viac ako 1700 hotových detekcií a viac ako 100 hotových dashboardov, ktoré sa dajú spustiť aj ako reporty. Všetky reporty sú „poháňané“ vyhľadávaním na pozadí a dajú sa upravovať.
	Systém SIEM musí tiež poskytovať reporty vo forme grafov a tabuliek	Áno. Všetky reporty vo Splunku sú „poháňané“ vyhľadávaním na pozadí a ako také sa dajú vizualizovať ako grafy, tabuľky, atď.
	Systém SIEM vytvára reporty vo formátoch PDF, JSON alebo iných	Áno. Splunk podporuje export reportov vo formátoch PDF, JSON, CSV, XML a surové dáta. https://docs.splunk.com/Documentation/Splunk/9.2.1/Search/ExportdatausingSplunkWeb
	Systém SIEM musí umožniť export údajov vo formáte XML alebo CSV	Áno. Splunk podporuje export reportov vo formátoch PDF, JSON, CSV, XML a surové dáta. https://docs.splunk.com/Documentation/Splunk/9.2.1/Search/ExportdatausingSplunkWeb
	Systém SIEM obsahuje analytické nástroje umožňujúce napríklad reportovanie, forenznú analýzu, analýzu zmien, štatistické reporty o aktuálnych aj historických údajoch.	Áno. Splunk ES ponúka komplexnú sadu analytických nástrojov, ktoré uľahčujú detailné reportovanie, forenznú analýzu, monitorovanie zmien a štatistické reportovanie o aktuálnych aj historických dátach. Jeho funkcie umožňujú analýzu v reálnom čase aj spätnú analýzu, zabezpečujú robustné riadenie bezpečnostných udalostí a dodržiavanie predpisov. Používatelia môžu generovať vlastné reporty, vizualizovať trendy dát a efektívne detegovať anomálie.
	Systém musí poskytovať report o aktivitách vybraných používateľov alebo skupín používateľov	Áno. Splunk ES umožňuje vyhľadávanie a reportovanie o aktivitách používateľov.
	Systém musí mať optimalizovanú databázu logov pre rýchle prehľadávanie a reportovanie (indexovanie).	Áno. Splunk používa ploché súbory a tsidx na indexovanie dát a umožňuje rýchle získavanie dát. Ponúkame funkcie ako „paralelné znižovanie spracovania vyhľadávania“, ktoré pomáha zrýchliť dokončovanie vyhľadávaní s vysokou kardinálnou hodnotou vo vašom nasadení platformy Splunk. Podporujeme tiež súhrnné indexy a zrýchlenie modelov dát pre veľmi rýchle získavanie historických dát. https://docs.splunk.com/Documentation/Splunk/9.2.1/DistSearch/Parallelreduceoverview https://docs.splunk.com/Documentation/Splunk/9.2.1/Knowledge/Configuresummaryindexes https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/Acceleratedatamodels
	Systém musí podporovať schopnosť zobraziť log záznam v jeho pôvodnej forme, ako bol prijatý, takzvaný "raw-message".	Áno. Splunk nemení prijaté logy a vždy umožňuje zobraziť surové logy tak, ako boli prijaté.
	Systém SIEM musí každému používateľovi poskytnúť vlastný personalizovaný dashboard	Áno. Vďaka výkonným funkciám RBAC môže mať každý používateľ svoj vlastný personalizovaný dashboard.
	Drill-down analýza v GUI, t. j. od všeobecnejších informácií vedú linky ku konkrétnejším informáciám (napr. z reportu o počte bezpečnostných udalostí podľa jednotlivých typov operačného systému je možné získať správu o počte bezpečnostných udalostí na jednotlivých hostoch s daným operačným systémom jedným kliknutím a ďalej pokračovať na report o počte bezpečnostných udalostí v jednotlivých aplikáciách/logoch/zdrojov na danom hoste, atď.).	Áno. Pri kliknutí používateľa na body dát, riadky tabuľky alebo iné prvky vizualizácie na dashboardu, môžete chcieť zdieľať ďalšie informácie. Použite funkciu drilldown na vytvorenie tejto interaktívnosti v dashboardoch. Drilldown je nástroj na konfiguráciu odpovedí na kliknutia používateľa na vizualizácie v dashboardu alebo formulári. Správanie drilldownu je konfigurované v jednotlivých vizualizáciách. Pre každú vizualizáciu v dashboardu môžete mať samostatné konfigurácie drilldownu. V závislosti od typu vizualizácie môžete tiež povoliť drilldown na špecifických prvkoch vo vizualizácii, ako je riadok alebo bunka tabuľky. https://docs.splunk.com/Documentation/Splunk/9.2.1/Viz/DrilldownIntro
	Systém musí podporovať automatické spúšťanie definovaných reportov (mesačne, týždenne, denne alebo v stanovenom čase), ukladanie na sieťovom úložisku a ich odosielanie e-mailom priamo zo systému.	Áno. Toto sa dosahuje pomocou uloženého vyhľadávania, ktoré sa môže spustiť podľa preddefinovaného harmonogramu (mesačne, týždenne, denne alebo v určený čas), uložiť tieto informácie a ktoré má nakonfigurovanú akciu upozornenia na napríklad odoslanie e-mailu s výsledkami.
Servisná podpora	Nepretržitá podpora v režime 24x7 s možnosťou zadať problém alebo incident priamo výrobcovi softvéru, alebo jeho certifikovanému partnerovi, s garantovanou dobou odozvy ma kritické incidenty do 2 hodín, po dobu 60 mesiacov od odovzdania v zmysle Zmluvy .	Nepretržitá podpora v režime 24x7 s možnosťou zadať problém alebo incident priamo výrobcovi softvéru, alebo jeho certifikovanému partnerovi, s garantovanou dobou odozvy ma kritické incidenty do 2 hodín, po dobu 60 mesiacov od odovzdania v zmysle Zmluvy .

Priložiť samostatnú tabuľku s podrobným rozpisom typu, produktového čísla, spôsobu licencovania a počtu dodávaných kusov aj s vyznačeným obdobím podpory pre ponúkaný softvér

Parameter	**Minimálne Požadované vlastnosti**	**Splnenie požadovaných vlastností uchádzačom (uchádzač uvedie konkrétne parametre ponukaného riešenia)**
Názov	**SOAR (Security orchestration, automation and response)**	**Výrobca: Cisco** **Model: Splunk SOAR - PH-T-LIC-U-ST**
Poradové číslo	**2**	**2**
Počet	**1**	**1**
Licencie	Požaduje sa dodať SOAR s licenciami pokrývajúcimi SIEM kapacitu, výkon a vlastnosti v položke 1. Pokiaľ je SOAR licencovaný na užívateľov požaduje sa dodať licencia pre 10 užívateľov.	Áno. Licencovanie Splunk SOAR je založené na „používateľských miestach“ a licencovaný používateľ nemá žiadne obmedzenia v tom, ako veľmi systém využíva (žiadne licenčné obmedzenia na použité integrácie, spustené API požiadavky, atď.). Viac informácií o licencovaní SOAR nájdete nižšie: https://docs.splunk.com/Documentation/SOARonprem/6.3.1/Admin/License#Seat-based_license
	Licencovanie a cena na riešení SOAR musí byť fixná, bez ohľadu na vyťaženie v časoch vysokého využitia SOAR	Áno. Licencovanie Splunk SOAR je založené na „používateľských miestach“ a licencovaný používateľ nemá žiadne obmedzenia v tom, ako veľmi systém využíva (žiadne licenčné obmedzenia na použité integrácie, spustené API požiadavky, atď.). Viac informácií o licencovaní SOAR nájdete nižšie: https://docs.splunk.com/Documentation/SOARonprem/6.3.1/Admin/License#Seat-based_license
Kompatibilita	SOAR musí byť plne kompatibilný s ponúkaným SIEM produktom.	Áno. Splunk ES (SIEM) a Splunk SOAR sú úzko integrované, čo umožňuje zákazníkom „testovať“ SOAR priamo z rozhrania Splunk ES, čím sa odstraňuje potreba, aby analytici pri svojej každodennej práci prihlasovali do rôznych nástrojov.
Integrácia	API rozhranie pre integráciu s existujúcimi bezpečnostnými nástrojmi a službami	Áno. Splunk SOAR ponúka množstvo dostupných REST API pre integráciu s nástrojmi tretích strán. https://docs.splunk.com/Documentation/SOARonprem/latest/PlatformAPI/Using
	Riešenie SOAR musí ponúkať knižnicu integrácií OOTB	Áno. Splunk ponúka niekoľko komunitných playbookov, vytvorených tímom Splunk alebo širšou komunitou, a dostupných pre všetkých zákazníkov Splunk SOAR: https://research.splunk.com/playbooks/
	Natívna integrácia s používanými produktmi Cisco Web Security Appliance, F5 BIG-IP Uchádzač priloží odkaz na webovú stránke kde je možné tieto integrácie overiť.	F5 BIG-IP LTM: https://splunkbase.splunk.com/app/5948 Cisco Web Security Appliance: integrácia OOTB momentálne nie je dostupná, ale dá sa vytvoriť zapojením partnera a/alebo Splunk PS Všetky integrácie OOTB pre Splunk SOAR nájdete tu: https://splunkbase.splunk.com/apps?page=1&filters=product%3Asoar
Automatizácia	Možnosť definovať a spúšťať automatizované bezpečnostné procesy a worklow.	Áno. Splunk SOAR umožňuje definovať a spúšťať automatizované bezpečnostné procesy a workflow vďaka Playbookom, ktoré orchestrajú a automatizujú všetky vaše bezpečnostné nástroje, čo umožňuje reagovať na incidenty strojovou rýchlosťou.
	Konfigurovateľné pravidlá na automatické spracovanie bezpečnostných udalostí a incidentov.	Áno. Splunk SOAR umožňuje nastaviť „aktívne“ playbooky, ktoré sa automaticky spúšťajú pri vašich bezpečnostných udalostiach/incidentoch na spracovanie, triáž a dokonca aj na odpovedanie strojovou rýchlosťou.
	Skripty a pluginy pre vlastné automatizované akcie.	Áno. Splunk SOAR umožňuje vkladať vlastný kód/skripty do našich Playbookov, čo poskytuje používateľom väčšiu flexibilitu a kontrolu. https://docs.splunk.com/Documentation/SOARonprem/latest/Playbook/CodeBlock
	Riešenie SOAR nesmie podporovať žiadne funkcie code/low code na vytváranie playbookov.	Áno. Splunk SOAR ponúka vizuálny editor playbookov (VPE), ktorý umožňuje zákazníkom vytvárať playbooky priamo z rozhrania, bez kódu. Upozorňujeme, že VPE umožňuje vlastný kód (python), ak je potrebný, ale filozofiou je znížiť túto potrebu čo najviac. https://www.splunk.com/en_us/resources/videos/splunk-soar-feature-overview-visual-playbook-editor-input-playbooks.html
	Riešenie SOAR musí na integráciu používať jednotný programovací jazyk.	Áno. Splunk SOAR používa Python pre integrácie a, ak si zákazníci želajú, aj pre kódovanie playbookov.
Reportovanie	Generovanie správ a štatistík o bezpečnostných incidentoch	Áno. Splunk SOAR umožňuje používateľom vytvárať súhrnné reporty a prezerať si všetky reporty vo Splunk SOAR. Zobraziť všetky reporty vytvorené alebo generované vo Splunk SOAR (On-premises) na stránke Reportovanie. Na tejto stránke môžete vykonať nasledujúce akcie: Zobraziť všetky dostupné reporty vo vašej inštancii Splunk SOAR (On-premises). Zobraziť iba reporty udalostí, ktoré sú reporty generované vo vnútri kontajnera. Zobraziť iba reporty prípadov, ktoré sú reporty generované vo vnútri prípadu. Zobraziť a vytvoriť súhrnné reporty. Súhrnné reporty môžete vytvárať iba na tejto stránke. https://docs.splunk.com/Documentation/SOARonprem/latest/User/Reporting
Správa	Viacúrovňové riadenie prístupu a práv používateľov.	Áno. Splunk SOAR ponúka výkonné možnosti RBAC prostredníctvom používania Rolí a Používateľov. Role vo Splunk SOAR (On-premises) slúžia na tieto účely: Udeliť používateľom povolenie na prístup k funkcionalite systému alebo obmedziť prístup k častiam systému. Slúžiť ako mechanizmus pre zoskupovanie používateľov pre schválenia. https://docs.splunk.com/Documentation/SOARonprem/latest/Admin/Roles
	Auditovateľnosť operácií a zmien v systéme.	Áno. Používatelia Splunk SOAR s príslušnými oprávneniami (t. j. administrátori) môžu upravovať platformu SOAR a jej fungovanie.
Servisná podpora	Nepretržitá podpora v režime 24x7 s možnosťou zadať problém alebo incident priamo výrobcovi softvéru, alebo jeho certifikovanému partnerovi, s garantovanou dobou odozvy ma kritické incidenty do 2 hodín, po dobu 60 mesiacov od odovzdania v zmysle Zmluvy .	Nepretržitá podpora v režime 24x7 s možnosťou zadať problém alebo incident priamo výrobcovi softvéru, alebo jeho certifikovanému partnerovi, s garantovanou dobou odozvy ma kritické incidenty do 2 hodín, po dobu 60 mesiacov od odovzdania v zmysle Zmluvy .

Priložiť samostatnú tabuľku s podrobným rozpisom typu, produktového čísla, spôsobu licencovania a počtu dodávaných kusov aj s vyznačeným obdobím podpory pre ponúkaný softvér

Názov Licencie	**Kvantita**	**Doba podpory**

Splunk Enterprise - Term License with Standard Success Plan - SE-T-LIC-ST	400 GB/day	**24 mesiacov + 12 mesiacov + 12 mesiacov + 12 mesiacov**
Splunk Enterprise Security - Term License with Standard Success Plan - ES-T-LIC-ST	400 GB/day	**24 mesiacov + 12 mesiacov + 12 mesiacov + 12 mesiacov**
Splunk SOAR - PH-T-LIC-U-ST - neobmedzený počet userov	1	**24 mesiacov + 12 mesiacov + 12 mesiacov + 12 mesiacov**