

Příloha č. 2

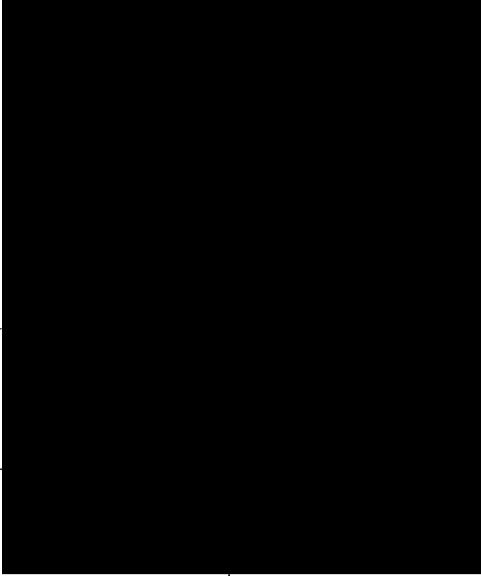
- ke Smlouvě na dodávku software dle GDPR pro počítačovou síť
nedílná součást zadávací dokumentace k podmínkám výzvy VZ 145.18

Cena - kalkulace

Nabídková cena za dodávku

Nabídková cena za dodávku představuje konečnou nepřekročitelnou cenu za dodávku software dle této smlouvy a je také použita *pro účely hodnocení ekonomické výhodnosti nabídky* dodavatele.

Součtová cenová kalkulace

typ	označení – popis – licence	Cena (bez DPH)	Cena (s DPH)
Dodávaný Systém	<i>Licence software včetně dokumentace a případné appliance pro příslušný software</i>		
Technická podpora	Technická podpora po dobu 5 let		
Implementace	Implementace dle rozsahu Implementace, nastavení a školení dle přílohy č. 1 smlouvy		
Celková cena dodávky		1 023 007,00 Kč	1 237 838,47 Kč

LEGENDA

Pro software dodávaného řešení se uvede „obchodní“ název a způsob licencování pro nabízenou cenu (*včetně ceny případné appliance pro příslušný software*). U nekomerčního sw se uvede 0 Kč. Podrobněji lze rozepsat dodávaný package dále v části Produkt/y (název, popis) této přílohy.

Software bude dodán s **technickou podporou na produkt po dobu 5 let, která zahrne minimálně:**

- zajištění nových verzí nebo subverzí software s vyšší nebo upravenou funkcionalitou na základě kontinuálního vývoje software,
- odstraňování vad programového vybavení
- průběžnou údržbu (aktualizaci) veškeré dokumentace vztahující se k dodanému programovému vybavení,
- periodické kontroly stavu systému
- kontrola incidentů v rozsahu 3 hod. měsíčně s písemným reportem zadavateli

Cena **implementace** do produkčního prostředí zahrnuje veškeré práce spojené s nastavením programového vybavení dle rozsahu instalace, viz příloha č.1 smlouvy.

Harmonogram dodávky

Pol.	Činnost	Trvání (dny)	OD (den od zahájení)	DO (den od zahájení)
1	zahájení	1	1	1
2	Analýza infrastruktury, stanovení metrik	3	2	4
3	Instalace a nastavení sw	14	5	18
4	akceptace	1	19	19
5	předání dodávky	1	20	20
6	ukončení	1	21	21

LEGENDA

Doba trvání je v pracovních dnech od zahájení, tj. účinnosti smlouvy.

Produkt/y (název, popis):

V moderní LAN infrastruktuře je nezbytné zaznamenávat události spojené s provozem.

Jedná se zejména o

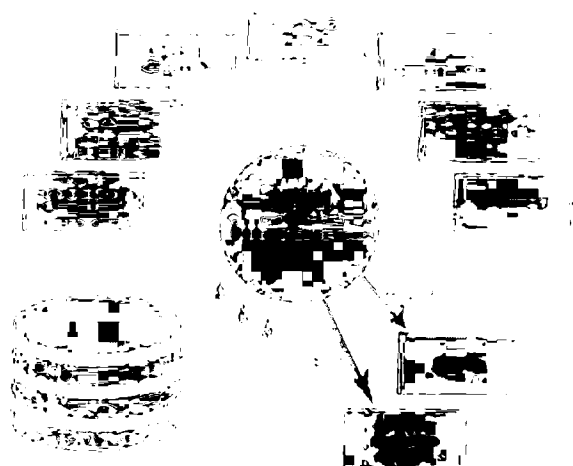
- Přístupy uživatelů k aktivním prvkům
- Konfigurační změny
- Systémové události na aktivních prvcích
- Bezpečnostní incidenty

Aktivní prvky mají tyto události zaznamenávat a automaticky odesílat nadřazenému systému. Pro komunikaci mezi aktivními prvky a centrálním logovacím systémem bývá nejčastěji používán protokol syslog.

Problémem však bývá spojit jednotlivé události z aktivních prvků do souvislostí. Díky potřebě uceleného pohledu nad událostmi v LAN byl po roce 2005 vyvinut systém SIEM (Security Information and Event Management), který poskytuje rozšířené funkcionality logování jako

- Agregace dat - seskupení vybrané části určitých entit za účelem vytvoření nové entity. Jednotlivými entitami mohou být např. data z přepínačů, firewallů, serverů, počítačových stanic, databází, IDS/IPS, aplikací atd.
- Korelace - nalézání vzájemných vztahů událostí, např. monitorování činnosti konkrétního uživatele, pohled na určité události v nějakém časovém intervalu atp.
- Varování (alerting)
- Informační panely, přehledové sestavy (dashboards)
- Reportování shod (compliance)
- Archivace, ukládání historických dat (logů)

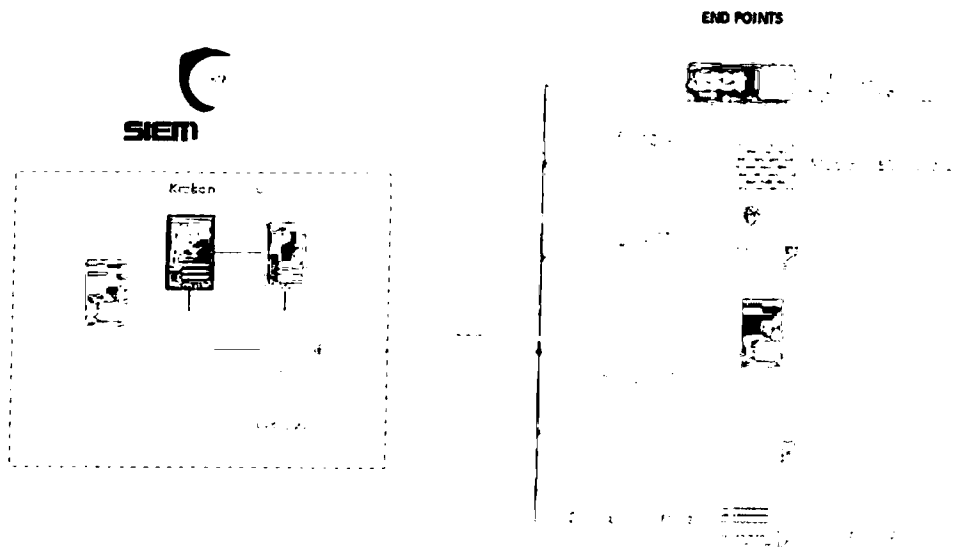
Tento nástroj umožňuje administrátorům pružnější a rychlejší reakce na útoky, včasnou detekci útoků a zefektivnění správy infrastruktury. Na systém SIEM je navíc možno směřovat logování dalších systémů (firewall, Flow monitoring, Active Directory ...), a tím zajistit komplexní přehled nad infrastrukturou LAN z jednoho místa.



Obrázek – Princip SIEM integrace

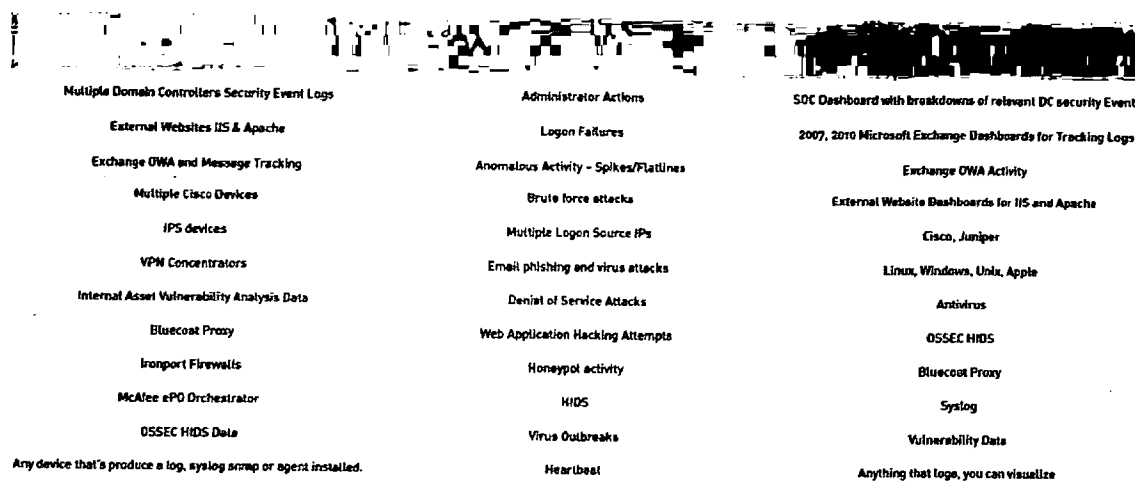
SIEMonster je komplexní Enterprise Security Information and Event Management (SIEM), postavený na škálovatelných, open-source součástech vyvinutých komunitou a týmem SIEMonster. SIEMonster byl vyvinut jako plná náhrada komerčních řešení SIEM. Produkt je pod Open-source licencí, plně zdokumentovaný, neexistují omezení dat nebo endpoint zařízení.

Architektura SIEM bude řešena 5-ti servery v clusteru (Makara, Kraken, Tiamat, Capricorn, Proteus) pojmenovaných podle mytologických postav.



- Makara - Orchestrator
- Proteus - Log kolektor
- Capricorn - Korelace a prohlížení logů
- Kraken - Database Cluster Node 1
- Tiamat - Database Cluster Node 2

SIEM - Přehled logovacích funkcí



Řešení je dimenzováno

- 1000 monitorovaných endpoint zařízení
- 47 mil událostí za hodinu cca 13 tis EPS (event per second)

Tento výkon je podmíněn 5-ti nodovým clusterem (4vCPU 2GHz, 8GB RAM) a uložištěm na SSD discích. Výkon lze škálovat přidáním dalších nodů do SIEM clusteru. Systém není licenčně omezen na počet logovaných endpoint zařízení nebo EPS

Aktivní prvky LAN (Router, Firewall, Switch, WIFI) podporující **syslog** zprávy budou předávat lokální logy SIEM syslog kolektoru, portem UDP/514 ev. TCP/514.

Windows servery odesílají lokální logy SIEM řešení prostřednictvím instalované služby **NXlog/Wazuh agent**. Tyto logy jsou parsovány, tříděny dle závažnosti a systémové ID události budou překládány do čitelné podoby.

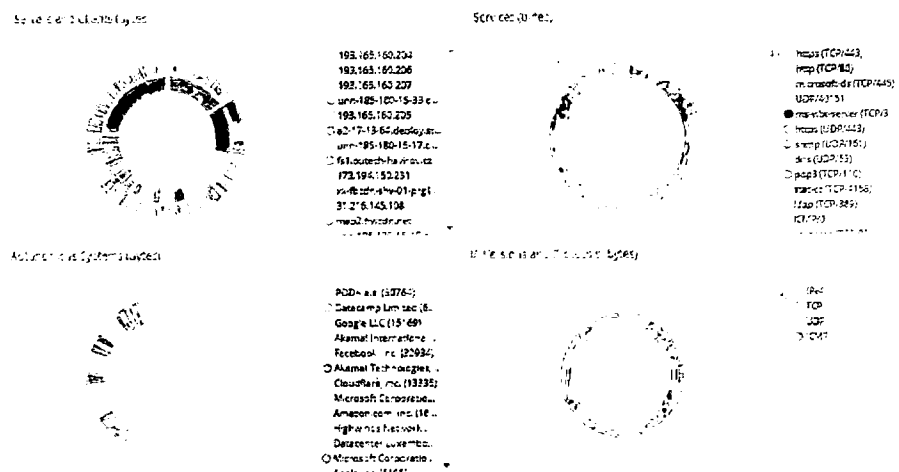
Linux server odesílají logy centrálnímu SIEM řešení prostřednictvím služby **filebeat/ Wazuh agent**.

Veškerá komunikace klientů se SIEM řešením (NXlog a filebeat a wazuh agent) probíhá šifrovaně, šifrování je řešeno SSL protokolem a certifikátem na endpoint zařízení.

Nasbírané aletry jsou ukládány v centrálním SIEM logu, kategorizovány dle typu provozu (windows/unix/syslog/aplikace ve standardizovaném formátu. Nad nasbíranými logy probíhá agregace a korelace dle přednastavených pravidel za účelem odhalení závadného provozu.

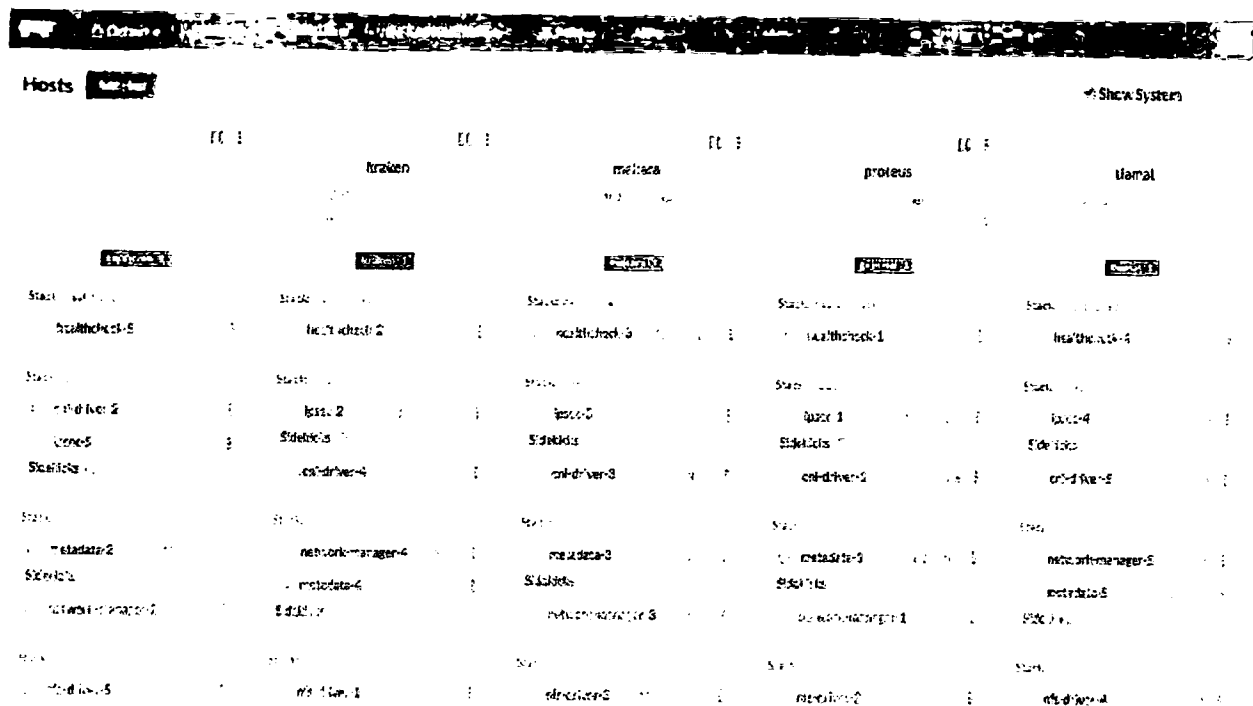
Vizualizace je řešena přehlednými grafy, tabulkami a sumárními pohledy nad logy.

Průchod paketu firewalllem (flow) je firewalllem zaznamenán a odeslán do SIEMu. Z jednotlivých flow jsou generovány statistiky o datových tocích a aktivitách uživatelů

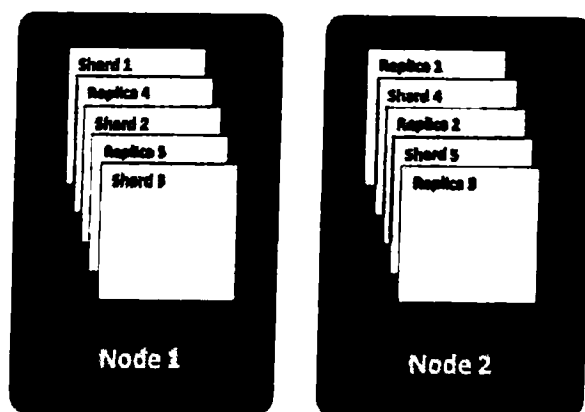


V databázi jednotlivých flow je možno dohledávat aktivitu jednotlivých uživatelů a serverů jak pro potřeby zpětné analýzy, tak i pro splnění požadavků GDPR.

Doporučené řešení je, implementovat celý systém do virtuálního prostředí VMware na samostatném HW serveru. V tomto případě bude systém implementován do stávajícího virtuálního prostředí zákazníka. Instalováno bude 5 severů na platformě Debian, případně jiné Linux distribuce. Každý server bude konfigurován 4vCPU, 8GB RAM, 50GB HDD. Jednotlivé servery budou clusterovány do SIEM řešení s jednotnou administrací přes webové rozhraní. Cluster bude provozován na platformě DOCKER. Redundance jednotlivých nodů a služeb bude zajištěna touto clusterizací a automatickým přebíráním rolí běžících na jednotlivých nodech clusteru.



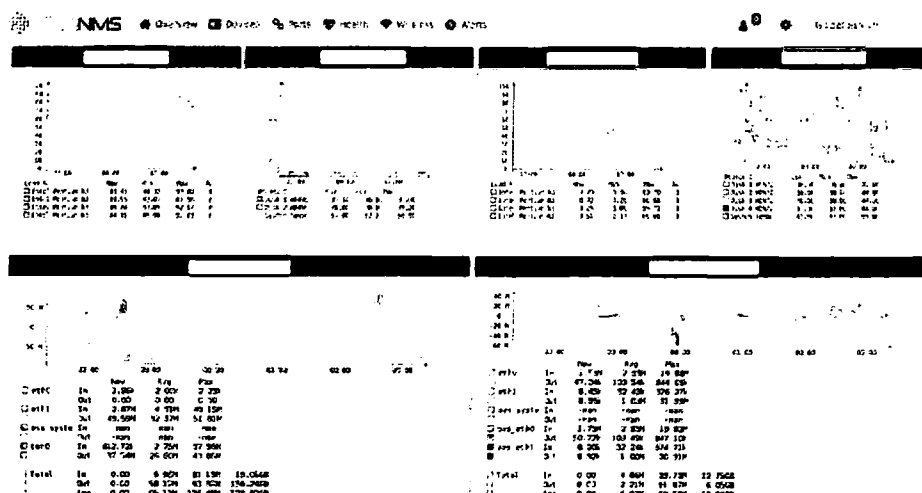
Ke clusteru bude připojeno pomocí NFS sdílené úložiště o velikosti 50GB sloužící pro sdílení konfigurací nad jednotlivými nody clusteru. Logy jsou ukládány v Elasticsearch (NO-SQL) databázi. Redundance dat je zajištěna křížovou replikací Elasticsearch databáze



Cluster 1

Služba bezpečnostního monitoringu je zabezpečena prostřednictvím školených pracovníků dodavatele, tzv. Security Operation Center.
Vitkovice IT Solution SOC, rozsah činností:

- Pro monitoring aktivních síťových prvků MÚ Ostrava Jih bude použit monitorovací nástroj NMS LibreNMS. Jedná se o open-source PHP/MySQL nástroj pro výkonnostní monitoring síťové infrastruktury.**



- Automatické autodiscovery - CDP, FDP, LLDP, OSPF, BGP, SNMP a ARP
- Automatické rozpoznání změny na aktivním prvku a promítnutí změny do monitorovaných služeb a tvorby přenosových statistik
- Vysoce flexibilní systém upozornění, upozornění prostřednictvím e-mailu, irc, SMS a další
- Plně zdokumentované API rozhraní pro správu a načítání dat z třetích aplikací
- Automatické aktualizace s opravami chyb, novými funkcemi a dalšími funkcemi
- Distribuované a škálovatelné řešení – vícenodové řešení
- Automatické tvorba síťových map dle závislostí mezi prvky, porty, IP adresami a ARP záznamy
- Webová administrace s napojením na LDAP a uživatelskými rolemi
- Automatické zálohování konfigurací síťových prvků
- Evidence IP adres a ARP záznamů z celé infrastruktury

Pro běh monitorovacího systému bude zapotřebí 4 vCPU, 4GB RAM a 100GB diskové kapacity. Systém bude instalován na operačním systému Debian 9. 64bit.