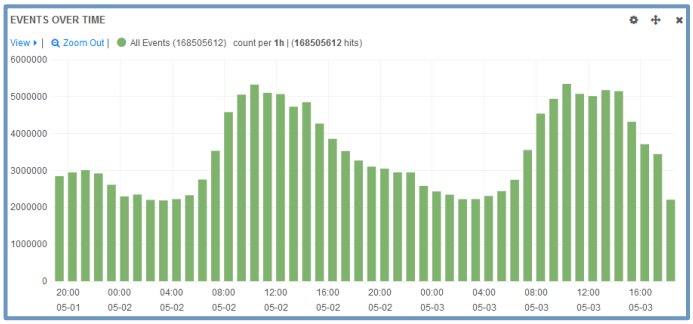
LOGmanager

> Centrální úložiště logů
> Dostupný SIEM

SPLŇUJE POŽADAVKY ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A GDPR

LOGmanager

V dnešnom pretechnizovanom svete sú informácie hlavným zdrojom umožňujúcim správne rozhodnutie v správny čas. Oproti tomuto konštatovaniu stojí fakt, že dôležité informácie sú distribuované cez najrôznejšie zariadenia a aplikácie naprieč celou organizáciou, nie vždy v ľahko pochopiteľnom formáte a s rozdielnou dostupnosťou. Zjednotenie informácií z viacerých zdrojov a ich preklad do ľudsky zrozumiteľného tvaru, nastavenie pravidiel na manipulovanie s informáciami a ich nespochybnenie sú preto kľúčovými požiadavkami na efektivitu bezpečnostných a operatívnych činností každej organizácie. Keď sa k tomu pridá aj prehľadná interpretácia týchto informácií v kompaktnom a výkonnom nástroji, získa IT organizácia nástroj pre realizáciu správnych rozhodnutí. A týmto nástrojom je český systém LOGmanager.



Určenie systému LOGmanager

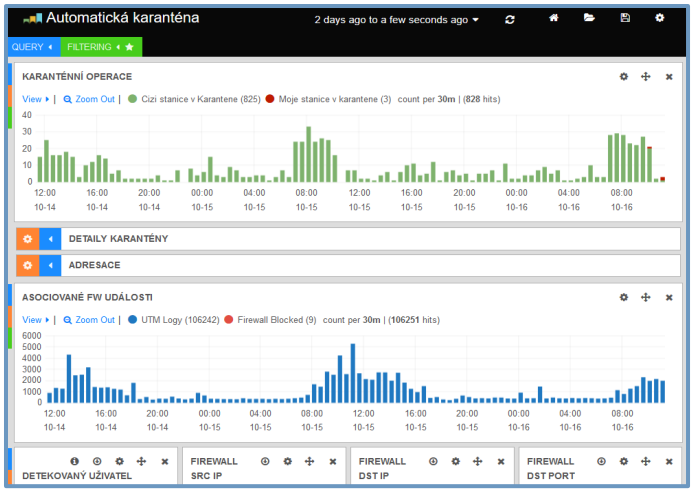
LOGmanager je HW riešenie na centralizovanú správu logov a iných strojových dát z ľubovoľných zdrojov. Je založený na výkonnej databáze s obrovskou kapacitou, rýchlym vyhľadávaním vo "veľkých dátach" a okamžitou vizualizáciou vyžiadaných dát. Jeho podstatou je zber, dlhodobo nespochybniteľné ukladanie a analýza strojových dát organizácie. Umožňuje prehľadávať agregované veľké dáta v reálnom čase, vytvárať štatistické analýzy, reporty a upozornenia na udalosti korelované z dát viacerých zdrojov. Nevyhnutnou súčasťou riešení LOGmanager je taktiež podpora súladu s požiadavkami zákonných noriem. Pri správnej implementácii pomôže organizácii so zaistením zhody s STN/ISO 27001:2013 o obstarávaní auditných záznamov, plnením požiadaviek GDPR či Zákona o kybernetickej bezpečnosti. LOGmanager však nie je určený iba pre oddelenie bezpečnosti IT alebo ako povinný nástroj k splneniu požiadavky regulácie. Pri vývoji LOGmanagera sa kladie veľký dôraz na jeho reálny prínos pre IT. Toto riešenie je veľkou pomocou pre prevádzku IT obecne, pretože na jednom mieste zhromažďuje prevádzkové dáta zo všetkých dôležitých systémov. Operátor IT tak má možnosť zistiť v priebehu pár sekúnd informácie o prevádzkových stavoch a prípadných poruchách, ktoré by inak musel hodiny komplikovane vyhľadávať v distribuovaných zdrojoch.

Podporované zariadenia

LOGmanager podporuje viac ako 125 zdrojov zo všetkých oblastí IT od bezpečnostných riešení cez sieťové prvky, virtualizáciu, operačné systémy, databázy až po cloud aplikácie. Zoznam je veľmi široký a s každou aktualizáciou sa rozširuje. LOGmanager podporuje štandardizované štruktúrované formáty logov CEF, LEEF, RFC5424 a JSON. Pre špecifické zdroje umožňuje rýchle a ľahké vytvorenie zákazníckych parserov.

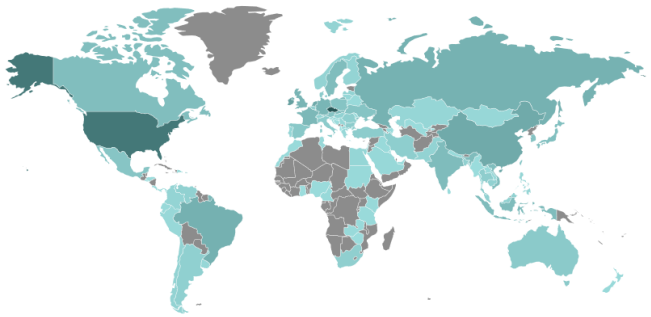
Kľúčové vlastnosti

- Centrálne úložisko logov, udalostí a strojových dát organizácie
- Zjednotenie formátu zdrojových logov do zrozumiteľnej formy
- Spracovanie a vizualizácia prijatých dát v reálnom čase
- Rýchle prehľadávanie dát bez nutnej znalosti SQL jazyka
- SIEM funkcie. Alerty na základe podmienok s limitmi a koreláciami
- Unikátne grafické konfiguračné a programovacie rozhranie
- Radikálna jednoduchosť a užívateľská prívetivosť
- Ľahké vytváranie reportov a auditných správ za behu
- Umožňuje ľahšie splnenie požiadaviek na zhodu s reguláciami pre:
  - GDPR
  - Zákon o kybernetickej bezpečnosti a nadväzujúce vyhlášky
  - STN/ISO 27001:2013 pre obstarávanie auditných záznamov
  - PCI DSS 3.2
- Bez licenčných obmedzení na množstvo zdrojov či uložené dáta
- Úspora na licenciách pri budúcom rozšírení smerom k SIEM/UBA



Konkurenčné výhody

- Trvalý príjem až 10 000 udalostí za sekundu
- Riešenie "všetko v jednom" - HW+SW na jednoduché nasadenie
- V základe diskové úložisko až pre 100TB logov
- Podpora veľkého množstva zdrojových zariadení, OS a aplikácií
- Centrálne riadený klient na zber logov z Windows OS
- Riešenie vysokej dostupnosti v Active/Active klastri
- Jednoduchá integrácia so SIEM/UBA systémami tretích strán
- Rýchle nasadenie a ľahké zaškolenie na bežné operácie
- Rozhranie a kompletná dokumentácia v českom aj anglickom jazyku
- Rozsiahla sieť spoľahlivých a technicky zdatných partnerov
- Priama technická podpora výrobcom a testovanie zadarmo



Typické užívateľské prípady

Zhoda s predpismi

Potrebujete vzhľadom na svoje pôsobenie centrálny systém na správu, analýzu a dlhodobé uloženie auditných i prevádzkových dát. Požadujete cenovo efektívne riešenie bez licenčných obmedzení, ktoré naplnia „tickboxy“ vo vašom auditnom pláne a firemnej bezpečnostnej politike...

Dohľad nad prístupom k sieti

Plánujete nasadiť centralizované riadenie prístupu k drôtovej a bezdrôtovej sieti a prevádzka IT potrebuje kontrolný systém pre 802.1X. Spojiť na jednom mieste logy z overovania na aktívnych prvkoch počítačovej siete, jednotného prihlásenia cez Active Directory, správy z RADIUS servera...

Dohľad nad súborovými servermi

Kto kopíroval alebo vymazal citlivé dáta zo súborových serverov? Chcete mať pod kontrolou operácie na súborových serveroch a vedieť, kedy, kto a aké operácie vykonával. Zasiahol vašu organizáciu ransomvér a chcete cielene obnoviť iba zašifrované súbory. Ale neviete, čo všetko bolo zašifrované...

Monitoring bezpečnosti

Chcete monitorovať bezpečnostné systémy, ale používate viaceré platformy, z ktorých by ste radi zjednotili logy a audity do jednotného formátu. Špecializované riešenie je veľmi drahé a má obmedzenú podporu iba pre niektorých výrobcov. LOGmanager spracuje a analyzuje logy zo všetkých zdrojov bez obmedzenia...

Prehľad konfiguračných zmien

Kto, kedy a s akým výsledkom vykonával konfiguračné zmeny v aktívnych prvkoch, operačných systémoch a aplikáciách. Potrebujete vždy čerstvé auditné dáta a reporty vo svojej e-mailovej schránke? Chcete vedieť, čo konkrétne administrátor pred polrokom modifikoval naprieč vaším IT...

Funkcie i ľahká integrácia

Obsahuje základné analytické funkcie SIEM riešenia. Ak sa však v budúcnosti rozhodnete pre nasadenie ďalšieho nástroja, LOGmanager pomôže. Umožňuje selektívne zdieľať štruktúrované dáta v mnohých formátoch s produktmi tretích strán. Šetrí tak na licenčných poplatkoch za tieto nástroje aj zjednoduší ich integráciu...

Kontrola pravidiel

Chcete overovať, či sú pravidlá v bezpečnostných systémoch v súlade s firemnou politikou...

Sledovanie prístupu k aplikáciám

Kto, kedy a s akým výsledkom vykonával operácie vo vašich aplikáciách a databázach...

Ochrana informácií

Strojové dáta nemožno modifikovať a vďaka certifikácii systému (STN/ISO 27001:2013) pre audit je možné LOGmanager použiť ako platformu na vytváranie reportov a forenznú analýzu...

Technická špecifikácia jednotlivých produktov LOGmanager

LOGmanager Appliance so softvérovou verziou 3.3.0 a novšou							
Procesor	Pamäť	Disk	RAID	Kapacita DB	Odhad retencie EPS[1] - dní	Trvalé EPS[1]	Špičkové EPS[1]
LOGmanager-XL na HPE alebo DELL serveri 2U výšky s Workload Akcelerátorom[2]. (5 rokov NBD RMA, 1 alebo 5 rokov SW aktualizácie, 1x LOGmanager-VF)							
2x14core Intel Xeon@2.6GHz	128GB	12*10TB	6	100TB	5 000 EPS - 365 dní	10,000	20 000/10 min.
LOGmanager-L na HPE alebo DELL serveri 2U výšky. (5 rokov NBD RMA, 1 alebo 5 rokov SW aktualizácie, 1x LOGmanager-VF)							
2x12core Intel Xeon@2.2GHz	128GB	12*4TB	6	40TB	3 000 EPS - 275 dní	5 000 (6 000[2])	10 000/10 min.
LOGmanager-M HPE alebo DELL server 1U výšky. (3 roky NBD RMA, 1 alebo 3 roky SW aktualizácie, 1x LOGmanager-VF)							
1x12core Intel Xeon@2.2GHz	64GB	4*4TB	5	12TB	1 000 EPS - 230 dní	2,000	4 000/10 min.
LOGmanager-S DELL Tower server. (3 roky NBD RMA, 1 alebo 3 roky SW aktualizácie, 1x LOGmanager-VF)							
1x2core Intel G5500@3.8GHz	32GB	2*4TB	1	4TB	250 EPS - 310 dní	500	1 000/10 min.
LOGmanager-Demo vo formáte Intel NUC - iba ako neprodukčný box pre lab alebo na PoC. (3 roky NBD RMA, 1 alebo 3 roky SW aktualizácie, 1x LOGmanager-VF)							
1x2core Intel i5@2.6GHz	32GB	1*500GB	N/A	490GB	250 EPS - 30 dní	500	1 000/10 min.
LOGmanager Forwarder (riešenie na bezpečný a spoľahlivý zber logov zo vzdialených pobočiek a z internetu/DMZ)							
Procesor	Pamäť	Disk	RAID	Kapacita DB	Odhad retencie	Trvalé EPS[1]	Špičkové EPS[1]
LOGmanager-VF Virtuálny forwarder s 8, 16 alebo 128 GB diskového priestoru vo verzii pre HyperV a VMWARE. (1 rok SW aktualizácie)							
2*vCPU	4GB vRAM	8/16/128GB vDisk	N/A	8/16/128GB	N/A; pracuje iba ako medzipamäť	9,000	18 000/10 min.
LOGmanager-HF Fyzický forwarder vo formáte Intel NUC. (3 roky NBD RMA, 1 rok SW aktualizácie)							
1x2core Intel i3@2.4GHz	8GB	120GB	N/A	120GB	N/A; pracuje iba ako medzipamäť	9,000	18 000/10 min.
LOGmanager Workload Accelerator[2] (Natívne integrovaný v LOGmanager-XL alebo ako voliteľné rozšírenie pre LOGmanager-L)							
LOGmanager-A Prídavný 3.2TB NVMe modul na akceleráciu spracovania near-realtime operácií **LOGmanager-XL** a **LOGmanager-L**.							
EPS[1] - očakávané množstvo udalostí za sekundu, Log mix s RAW veľkosťou logov priemerne 700 Byte. Odhad retencie pre nonstop spracovanie daného objemu EPS.							

Informácie o výrobcovi a referencie

LOGmanager sa vyvíja od roku 2014 ako nosný produkt firmy Sirwisa, a.s., ktorá sídli v Prahe. Doteraz našiel LOGmanager viac ako 160 spokojných zákazníkov a na stránkach www.logmanager.sk nájdete vybrané referencie. Medzi našich zákazníkov patrí nielen štátna správa, ale aj priemyselné podniky všetkých veľkostí a odvetví, obchodné spoločnosti, banky, poisťovne a ďalšie. Ohľadom ďalších referencií priamo z oblasti, ktorá vás zaujíma, nás neváhajte kontaktovať. Príslušné kontakty na existujúcich zákazníkov, ktorí súhlasia s uvádzaním na referenčnom liste, radi poskytneme.