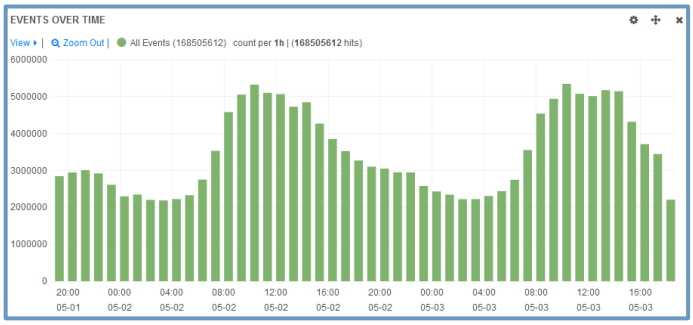
LOGmanager

> 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 preloženie do ľudsky zrozumiteľného tvaru, nastavenie pravidiel pre manipulovanie s informáciami a ich nespochybnenie sú preto kľúčovými požiadavkami pre 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

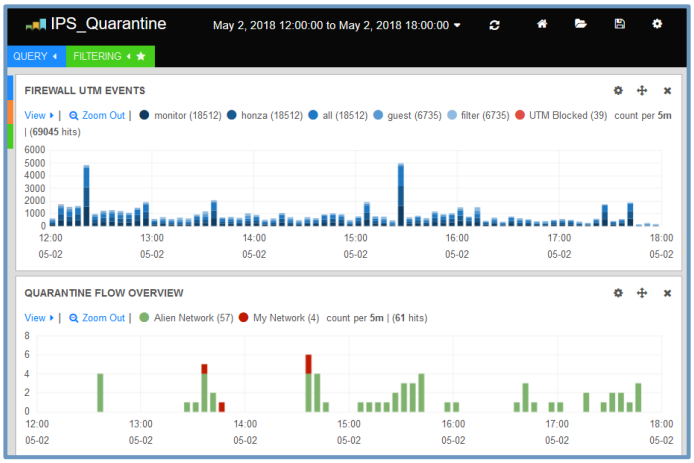
LOGmanager je HW riešenie pre centralizovanú správu logov a iných strojových dát z ľubovoľných zdrojov. Je založený na výkonnej databáze s obrovskou kapacitou, rýchlym vyhľadávaním vo "veľkých dátach" a okamžitou vizualizáciou vyžiadaných dát. Jeho podstatou je zber, dlhodobo nespochybniteľné ukladanie 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 k zaisteniu zhody s STN/ISO 27001:2013 o obstarávaní auditných záznamov, plnenie požiadaviek GDPR či Zákona o kybernetickej bezpečnosti. LOGmanager však nie je určený iba pre oddelenie bezpečnosti IT, alebo ako povinný nástroj k splneniu diskutabilnej požiadavky nejakej regulácie. Pri vývoji LOGmanagera je kladený 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 dostane 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 120 zdrojov zo všetkých oblastí IT, od bezpečnostných riešení, cez sieťové prvky, virtualizáciu, operačné systémy, databázy až po aplikácie. Zoznam je veľmi široký a s každou aktualizáciou sa rozširuje. LOGmanager ďalej podporuje štandardizované štruktúrované formáty logov ako sú CEF, LEEF a JSON. Pre špecifické zdroje umožňuje rýchle a ľahké vytvorenie zákazníckych parserov.

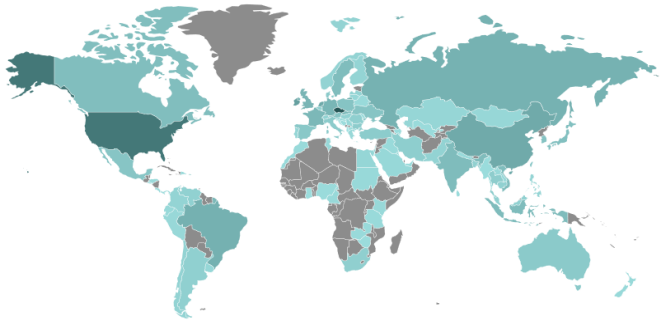
Kľúčové vlastnosti

- 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 pre základné aj pokročilé operácie, vždy v grafickom prostredí
- 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



Konkurenčné výhody

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



Typické užívateľské prípady

Zhoda s predpismi

Potrebujete vzhľadom k svojmu pôsobeniu centrálny systém pre 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...

Dozor 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 emailovej schránke? Chcete mať možnosť vedieť, čo konkrétne administrátor pred pol rokom modifikoval naprieč Vaším IT...

Ochrana informácií

Ochrana informácií proti neoprávnenému vymazaniu či modifikácii. Logy, strojové dáta a udalosti v LOGmanageri nie je možné modifikovať a vďaka certifikačnému systému podľa STN/ISO 27001:2013 pre obstarávanie auditných záznamov je možné LOGmanager použiť ako platformu pre vytvorenie dôkazov o činnostiach, operáciách...

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...

Identifikácia dátových tokov

Kto z externistov sťahoval cez VPN viac dát z Vašej siete, ako je obvyklé. Z akých zdrojov a čo presne vyniesol ...

Technická špecifikácia jednotlivých produktov LOGmanager

LOGmanager Appliance se software 3.x							
Procesor	Paměť	Disk	RAID	Kapacita DB	Odhad retence EPS[1] - dní	Trvalé EPS[1]	Špičkové EPS[1]
LOGmanager-XL na HPE nebo DELL serveru 2U výšky s integrovaným Workload Akcelerátorem[2]. (5 let NBD RMA, 1 nebo 5 let SW aktualizace, 1x LOGmanager-VF)							
2x14core Intel Xeon@2.6GHz	128GB	12*10TB	6	100TB	5000EPS - 365dní	10000	20000/10min
LOGmanager-L na HPE nebo DELL serveru 2U výšky. (5 let NBD RMA, 1 nebo 5 let SW aktualizace, 1x LOGmanager-VF)							
2x10core Intel Xeon@2.2GHz	128GB	12*4TB	6	40TB	3000EPS - 275dní	5000 (6000[2])	10000/10min
LOGmanager-M HPE nebo DELL server 1U výšky. (3 roky NBD RMA, 1 nebo 3 roky SW aktualizace, 1x LOGmanager-VF)							
1x10core Intel Xeon@2.2GHz	64GB	4*4TB	5	12TB	1000EPS - 230dní	2000	4000/10min
LOGmanager-Demo ve formátu Intel NUC - pouze jako neprodukční box pro lab nebo na PoC. (3 roky NBD RMA, 1 nebo 3 roky SW aktualizace, 1x LOGmanager-VF)							
1x2core Intel i5@2.9GHz	16GB	1*500GB	N/A	490GB	250EPS - 30dní	500	1000/10min
LOGmanager Forwarder (řešení pro bezpečný a spolehlivý sběr logů ze vzdálených poboček a z Internetu/DMZ)							
Procesor	Paměť	Disk	RAID	Kapacita DB	Odhad retence	Trvalé EPS[1]	Špičkové EPS[1]
LOGmanager-VF Virtuální forwarder s 8, 16 nebo 128GB diskového prostoru ve verzi pro HyperV a VMWARE. (1 rok SW aktualizace)							
2*vCPU	4GB vRAM	8/16/128GB vDisk	N/A	8/16/128GB	N/A; pracuje pouze jako mezipaměť	9000	18000/10min
1*vCPU	4GB vRAM	8/16/128GB vDisk	N/A	8/16/128GB	N/A; pracuje pouze jako mezipaměť	6000	12000/10min
LOGmanager-HF Fyzický forwarder ve formátu Intel NUC. (3 roky NBD RMA, 1 rok SW aktualizace)							
1x2core Intel i5@2.9GHz	16GB	500GB	N/A	490GB	N/A; pracuje pouze jako mezipaměť	9000	18000/10min
LOGmanager Workload Accelerator[2] (Nativně integrován v LOGmanager-XL nebo jako volitelné rozšíření pro LOGmanager-L)							
LOGmanager-A Přídavný 3.2TB NVMe modul k akceleraci zpracování near-realtime operací **LOGmanager-XL** a **LOGmanager-L**.							
EPS[1] - očekávané množství události za sekundu, Log mix s RAW velikostí logů průměrně 700Byte. Odhad retence - kalkulace pro 24hodinové zpracování daného objemu EPS.							

Informácie o výrobcovi a referencie

LOGmanager je vyvíjaný od roku 2014 ako nosný produkt firmy Sirwisa a.s., ktorá sídli v Prahe. Doteraz našiel LOGmanager viac ako 120 spokojných zákazníkov a na stránkach www.logmanager.sk nájdete vybrané referencie. Medzi našich zákazníkov patrí nielen štátna správa, ale aj priemyslové podniky všetkých veľkostí a oborov, obchodné spoločnosti, banky, poisťovne a ďalšie. Pre ďalšie referencie priamo z oblasti, ktorá Vás zaujíma nás neváhajte kontaktovať. Príslušné kontakty na existujúcich zákazníkov, ktorí súhlasia s uvádzaním na referenčnom liste, radi poskytneme.