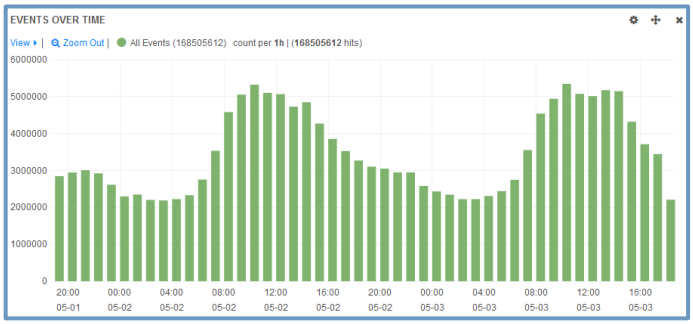
LOGmanager

> Centrální úložiště logů
> Dostupný SIEM

SPLŇUJE POŽADAVKY ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A GDPR

LOGmanager

V dnešním přetechnizovaném světě jsou informace kritickým zdrojem umožňujícím správné rozhodnutí ve správný čas. V protikladu k tomu konstatování stojí fakt, že důležité informace jsou distribuovány v nejrůznějších zařízeních a aplikacích napříč celou organizací, ne vždy ve snadno pochopitelném formátu a s rozdílnou dostupností. Sjednocení informací z mnoha zdrojů a jejich přeložení do lidsky srozumitelného tvaru, nastavení pevných pravidel pro nakládání s informacemi a jejich nezpochybnitelnost jsou proto klíčové požadavky pro efektivitu bezpečnostních i operativních činností každé organizace. Když se k tomu přidá i přehledná interpretace těchto informací v kompaktním a výkonném nástroji, získá IT organizace nástroj pro realizaci správných rozhodnutí. A tímto nástrojem je český systém LOGmanager.



Určení systému LOGmanager

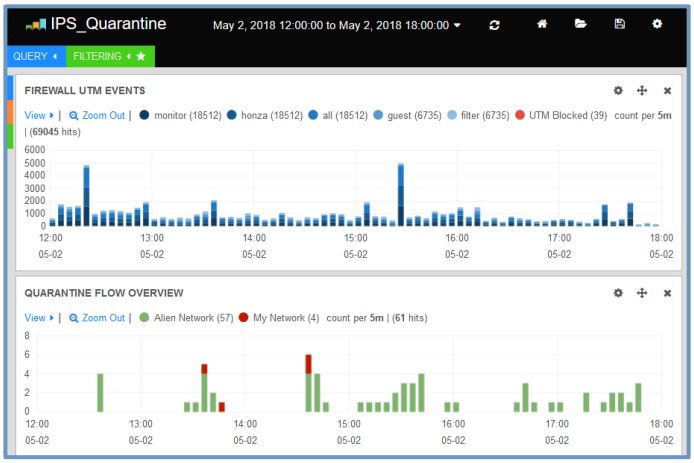
LOGmanager je HW řešení pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů. Je založen na výkonné databázi s obrovskou kapacitou, rychlým vyhledáváním ve "velkých datech" a okamžitou vizualizací vyžádaných dat. Jeho podstatou je sběr, dlouhodobé nezpochybnitelné ukládání a analýza strojových dat organizace. Umožňuje prohledávat agregovaná velká data v reálném čase, vytvářet statistické analýzy, reporty a upozornění na události korelované z dat více zdrojů. Nedílnou součástí řešení LOGmanager je taktéž podpora souladu s požadavky zákonných norem. Při správné implementaci pomůže organizaci k zajištění shody s ČSN/ISO 27001:2013 o pořizování auditních záznamů, plnění požadavků GDPR či Zákona o kybernetické bezpečnosti. LOGmanager však není určen pouze pro oddělení bezpečnosti IT, nebo jako povinný nástroj ke splnění diskutabilního požadavku nějaké regulace. Při vývoji LOGmanageru je kladen velký důraz na jeho reálný přínos pro IT. Toto řešení je velkou pomocí pro provoz IT obecně, protože na jednom místě shromáždí provozní data ze všech důležitých systémů. Operátor IT tak dostane možnost zjistit během několika sekund informace o provozních stavech a případných závadách, které by jinak musel hodiny komplikovaně vyhledávat v distribuovaných zdrojích. K tomu je i automaticky informován o sledovaných událostech a může tak předcházet kritickým IT nebo bezpečnostním incidentům.

Podporovaná zařízení

LOGmanager nativně podporuje více než 120 zdrojů ze všech oblastí IT, od bezpečnostních řešení, přes síťové prvky, virtualizace, operační systémy, databáze až po aplikace. Seznam je velmi široký a s každou aktualizací se rozšiřuje. LOGmanager dále podporuje standardizované strukturované formáty logů jako jsou CEF, LEEF a JSON. Pro specifické zdroje umožňuje rychlé a snadné vytvoření zákaznických parserů.

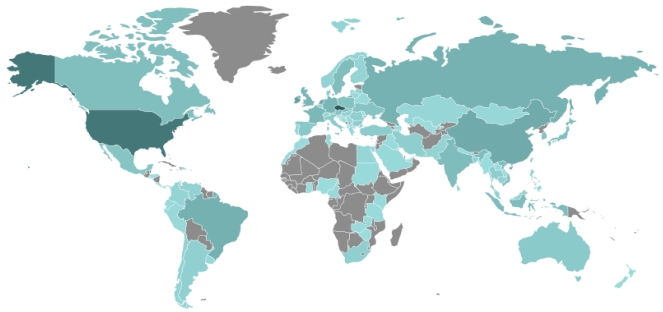
Klíčové vlastnosti

- Centrální úložiště logů, událostí a strojových dat organizace
- Sjednocení formátu zdrojových logů do lidsky srozumitelné formy
- Zpracování a vizualizace přijímaných dat v reálném čase
- Rychlé prohledávání dat bez nutnosti znalosti SQL jazyka
- SIEM funkce. Alerty na základě podmínek s limity a korelacemi
- Unikátní grafické konfigurační a programovací rozhraní
- Radikální jednoduchost a uživatelská přívětivost pro základní i pokročilé operace, vždy v grafickém prostředí
- Snadné vytváření reportů a auditních zpráv za běhu
- Umožní snadnější splnění požadavku na shodu s regulacemi pro:
  - GDPR
  - Zákon o kybernetické bezpečnosti a návazné vyhlášky
  - ČSN/ISO 27001:2013 pro pořizování auditních záznamů
  - PCI DSS 3.2
- Bez licenčních omezení na množství zdrojů, výkon a uložená data



Konkurenční výhody

- Trvalý příjem až 10 000 událostí za sekundu
- Řešení „vše v jednom" - Server, OS, Aplikace, DB na jedné platformě
- V základu diskové úložiště pro až 100TB logů
- Podpora velkého množství zdrojových zařízení, OS a aplikací
- Centrálně řízený klient pro sběr logů z Windows OS
- Možnost vysoké dostupnosti v Active/Active clusteru
- Rychlé nasazení a snadné zaškolení pro běžné operace
- Rozhraní i kompletní dokumentace v českém jazyce
- Navrženo s ohledem na specifika středoevropských zemí
- Rozsáhlá síť spolehlivých a technicky zdatných partnerů
- Přímá technická podpora výrobcem a možnost testování zdarma



Typické uživatelské případy

Shoda s předpisy

Potřebujete vzhledem ke svému působení centrální systém pro správu, analýzu a dlouhodobé uložení auditních i provozních dat. Požadujete cenově efektivní řešení bez licenčních omezení, které naplní „tickboxy" ve Vašem auditním plánu a firemní bezpečnostní politice...

Dohled nad přístupem k síti

Plánujete nasadit centralizované řízení přístupu k drátové a bezdrátové síti a provoz IT potřebuje dohledový systém pro 802.1X. Spojit na jednom místě logy z ověřování na aktivních prvcích počítačové sítě, jednotného přihlášení přes Active Directory, zprávy z RADIUS serveru...

Dohled nad souborovými servery

Kdo kopíroval nebo mazal citlivá data ze souborových serverů? Chcete mít pod kontrolou operace na souborových serverech a vědět kdy, kdo a jaké operace prováděl. Zasáhl vaši organizaci Ransomware a chcete cíleně obnovit pouze zašifrované soubory. Ale nevíte, co bylo zašifrováno...

Monitoring bezpečnosti

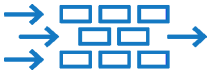
Chcete monitorovat bezpečnostní systémy, ale používáte více platforem, ze kterých byste rádi sjednotili logy a audity do jednotného formátu. Specializované řešení je moc drahé a má omezenou podporu pouze pro některé výrobce. LOGmanager zpracuje a analyzuje logy ze všech zdrojů bez omezení...

Sledování konfiguračních změn

Kdo, kdy a s jakým výsledkem prováděl konfigurační změny v aktivních prvcích, operačních systémech a aplikacích. Potřebujete vždy čerstvá auditní data a reporty ve své emailové schránce? Chcete mít možnost vědět, co konkrétní administrátor před půl rokem modifikoval napříč Vaším IT...

Ochrana informací

Ochrana informací proti neoprávněnému smazání či modifikaci. Logy, strojová data i události v LOGmanageru nelze modifikovat a díky certifikaci systému dle ČSN/ISO 27001:2013 pro pořizování auditních záznamů lze LOGmanager použít jako platformu pro vytvoření důkazů o činnostech, operacích...



Kontrola pravidel

Chcete ověřovat, zda jsou pravidla v bezpečnostních systémech v souladu s firemní politikou...

Sledování přístupu k aplikacím

Kdo, kdy a s jakým výsledkem prováděl operace ve Vašich aplikacích a databázích...

Identifikace datových toků

Kdo z externistů stahoval přes VPN více dat z Vaší sítě, než je obvyklé. Z jakých zdrojů, co přesně vynesl...

Technická specifikace jednotlivých produktů 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.							

Informace o výrobci a reference

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Do vydání tohoto produktového listu nalezl LOGmanager více jak 120 spokojených zákazníků a na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější reference přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.