LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Prípadová štúdia - Univerzita Konštantína Filozofa v Nitre

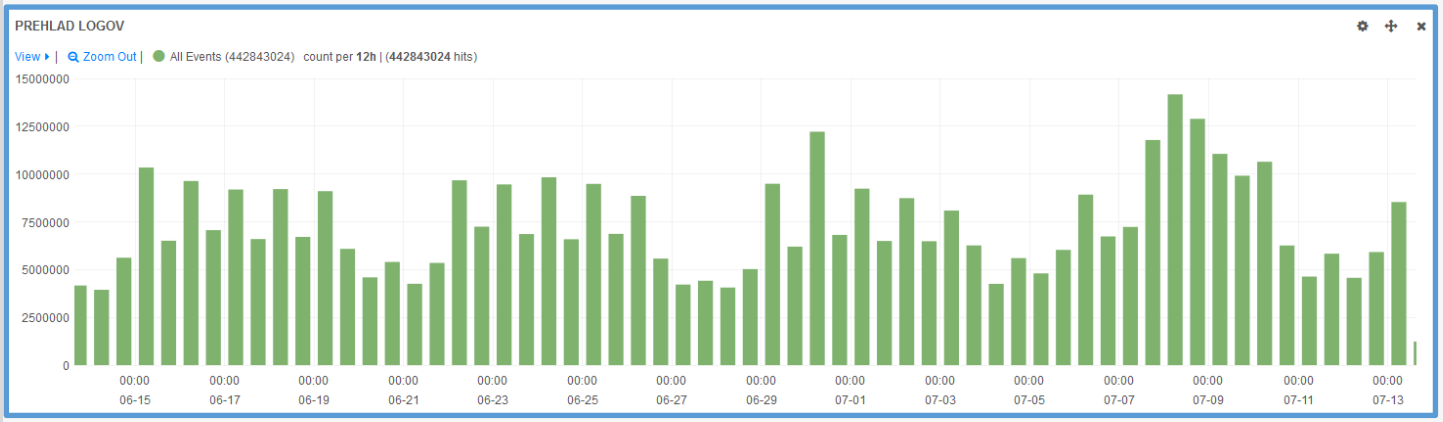
O zákazníkovi

Univerzita Konštantína Filozofa v Nitre je univerzitná verejná vysoká škola, ktorej poslaním je rozvíjať harmonickú osobnosť, vedomosti, múdrosť, dobro a tvorivosť v človeku a prispievať tak k rozvoju vzdelanosti, vedy, kultúry a zdravia pre blaho celej spoločnosti. Hlavnou úlohou UKF pri napĺňaní jej poslania je poskytovanie vysokoškolského vzdelávania a tvorivé vedecké bádanie alebo tvorivá umelecká činnosť.

Univerzita pozostáva z piatich fakúlt a ako inštitúcia je rozmiestnená v 12 objektoch alokovaných v rôznych častiach mesta Nitra. Univerzita okrem výchovy vlastných študentov participuje na vzdelávaní a príprave učiteľov slovenskej národnosti žijúcej v zahraničí, uskutočňuje doktorandské štúdium v schválených študijných programoch, udeľuje /akademické a vedecko-pedagogické tituly a uskutočňuje ďalšie vzdelávanie.

Čo zákazníka najviac trápilo?

Pri správe takého rozsiahleho a komplikovaného IT prostredia, aké má vo svojej pôsobnosti IT oddelenie UKF, je najčastejším problémom rýchlosť a zložitosť získania potrebných informácií. Nesmieme zabudnúť na fakt, že v prostredí, kde sa pohybuje niekoľko tisíc užívateľov (profesorov, študentov a iný personál), sa každú chvíľu objaví bezpečnostný incident. Ak sa ihneď nevyrieši, ohrozí vzdelávací a výskumný proces na univerzite. Preto sa rozhodli pre kritickú infraštruktúru zaviesť centrálnu logovaciu platformu, na ktorej sú schopní rýchlo a efektívne vyhľadať požadované informácie a následne zamedziť akejkoľvek neželanej činnosti, výpadkom či nebodaj odcudzeniu časti infraštruktúry.



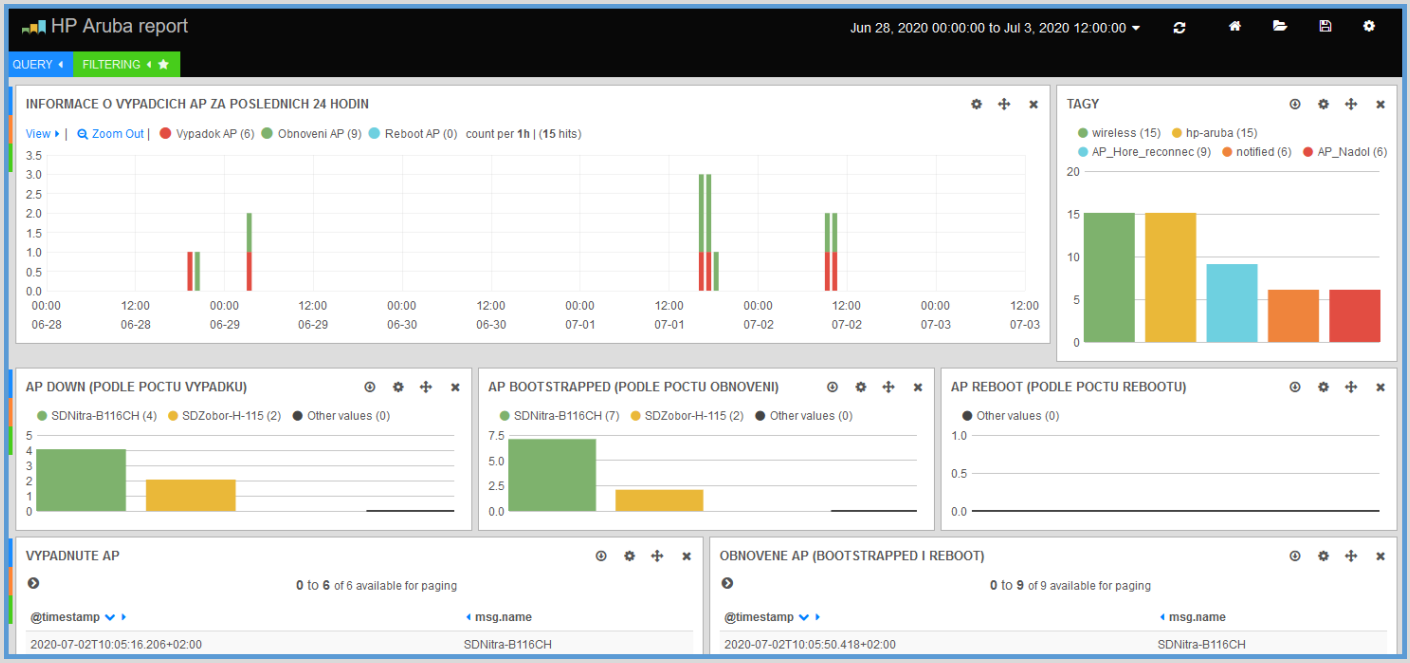
Nasadenie LOGmanagera v prostredí UKF

Milan Oravec, pracovník CIKT UKF Nitra:

LOGmanager sme si u nás na UKF vyskúšali v rámci PoC. Vďaka tomu sme vedeli, čo všetko môžeme v reálnej prevádzke očakávať a kde všade budeme môcť využiť potenciál tejto inteligentnej a užívateľsky veľmi prívetivej platformy v našom prostredí. Vzhľadom na bezpečnosť a ochranu osobných údajov uvediem 2 príklady využitia LOGmanagera u nás.

I. Príklad

Keďže máme svoju infraštruktúru inštalovanú aj vo verejných priestoroch, napr. študentské internáty, mali sme z času na čas problém s jej "miznutím". Vďaka LOGmanageru máme vytvorené upozornenia, ktoré informujú zodpovedných technikov. V prípade "zmiznutia" zariadenia následne preveria, či ide o poruchu alebo o krádež. Vďaka LOGmanageru vieme o týchto situáciách okamžite.



II. Príklad

UKF ako člen akademickej obce si nemôže dovoliť tolerovať akúkoľvek nezákonnú činnosť svojich užívateľov. Máme nastavené rôzne ochranné mechanizmy. Napriek tomu sa však občas stane, že niektorým užívateľom sa podarí niečo "vyviesť" a je našou povinnosťou ich vypátrať a zamedziť tejto činnosti. Vďaka LOGmanageru nemusíme prácne manuálne prehľadávať niekoľko systémov a logov. Všetky potrebné informácie totiž máme na jednom centrálnom mieste v LOGmanageri, kde sa vďaka pár kliknutiam dokážeme veľmi rýchlo dopracovať k informácii o konkrétnom previnilcovi.

Pre nedostatok miesta nahrádzame screenshot komentárom výrobcu: LOGmanager v jednom zobrazení asociuje logmi z 3 systémov - Firewallu, DHCP servera a FreeRadius servera. Tieto služby bežia na samostatných Linux serveroch. Na nájdenie užívateľa porušujúceho pravidlá stačí zvyčajne zvoliť vo firewall logu cieľovú IP adresu, pre ktorú je hlásené porušenie pravidiel. LOGmanager v priebehu sekúnd zobrazí príslušné logy z firewallu a asociované logy z DHCP. Zvolením zdrojové MAC adresy identifikovaného útočníka v logu DHCP servera sa administrátor dostane okamžite k identite užívateľa vo Freeradius servery. Operácia, ktorá predtým trvala desiatky minút prácneho prehľadávania textových logov, je teraz záležitosťou sekúnd.

PRÍNOS PRE ZÁKAZNÍKA A OCEŇOVANÉ VLASTNOSTI

Zákazník najviac ocenil možnosť odskúšania platformy LOGmanagera vo svojej infraštruktúre a následný jednoduchý prechod do ostrej prevádzky. LOGmanager so svojím užívateľsky jednoduchým rozhraním šetrí čas správcov, operátorov a pomáha im rýchlejšie a efektívnejšie spracovať IT incidenty. Navyše ho potešilo, že sa nemusí obávať žiadnych dodatočných nákladov v prípade nárastu zalogovaných udalostí, keďže LOGmanager nemá žiadne licenčné obmedzenie na počet zalogovaných udalostí.

INFORMÁCIE O VÝROBCOVI A ĎALŠIE REFERENCIE

LOGmanager sa vyvíja od roku 2014 ako nosný produkt firmy Sirwisa, a.s., ktorá sídli v Prahe. Na stránkach www.logmanager.cz/.sk/.pl/.com nájdete vybrané referencie. Medzi našich zákazníkov patrí nielen štátna správa, ale aj priemyselné podniky všetkých veľkostí, obchodné spoločnosti, spoločnosti z oblasti bankovníctva, školstva, zdravotníctva a ďalšie. Ohľadom podrobnejšieho zoznamu priamo z oblasti vašej činnosti nás neváhajte kontaktovať.