Nasazení a provoz centrálního systému na správu a analýzu logů

Důvodová zpráva s argumenty pro nasazení SEM-SIEM řešení včetně uživatelských příkladů

Existují tři základní důvody, pro které organizace zvažují nasazení systému pro centralizovanou správu a analýzu logů. Jsou z těchto oblastí a každá může mít v organizaci dle jejího zaměření rozdílnou váhu:

- Provozní a operační
- Bezpečnostní
- Dodržení souladu s regulacemi a audit

V následujícím popisu jsou rozvedeny jednotlivé oblasti s konkrétními případy možného praktického použití LOGmanageru pro danou agendu. Možnosti použití jsou samozřejmě podstatně širší, vzorek uživatelských případů je pouze ilustrativní pro vytvoření základní představy.

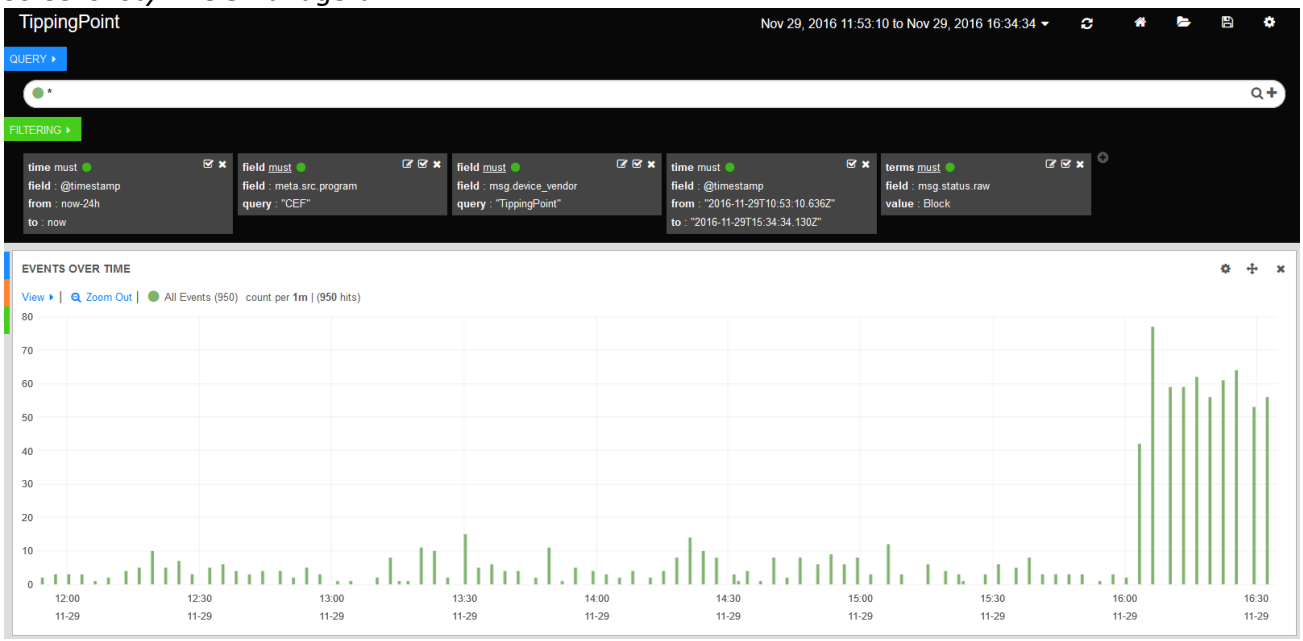
Provozní a operační oblast

Kritický IT incident je středobodem dnešního IT světa, je nevyhnutelný stejně jako daně a smrt, protože dříve či později přijde. První, co znamená kritický IT incident – je to stav, kdy je nefunkční business aplikace nebo infrastruktura, na které je kritická aplikace navázaná. Taková situaci vyžaduje okamžité řešení, při kterém členové IT teamu organizace dle charakteru incidentu spolupracují na urychleném odstranění závady. V této souvislosti se zažily dva pojmy – MTTR a RCA (Mean Time To Repair a Root Cause Analysis; volně přeloženo to znamená Střední doba k nápravě a Analýza příčin problému). Snahou IT oddělení je najít co nejdříve příčinu výpadku a odstranit ji, poté analyzovat proč k výpadku došlo včetně souvislostí, zhodnotit celý incident a určit opravné mechanismy, aby ke stejné nebo podobné závadě příště nedošlo.

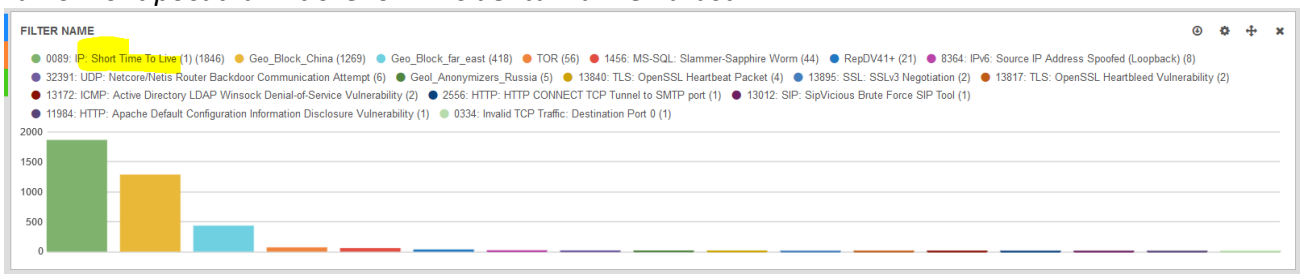
***Příklad použití LOGmanageru z praxe pro Kritický IT incident**: Známe přibližný čas počátku výpadku, aktuálně nic vyjma broadcast domén nekomunikuje. V LOGmanageru – dashboardu „All Event Overview" si vybereme příslušný časový úsek plus mínus 5 minut. Vybereme major a critical events a zahájíme průzkum logů z tohoto výběru od počátku časového úseku. Během procházení logů zjistíme, že centrální router ztratil spojení se svými OSPF partnery a že se rozpadlo směrování. A to včetně linek směrem ke vnitřním DNS serverům. Nedošlo však ke ztrátě fyzických linek ani k přepočítávání v síťových protokolech druhé vrstvy (MSTP, LLDP). Zrušíme výběr major a critical events a soustředíme se na informace, které předcházejí rozpadu OSPF. V intervalu předcházejícímu rozpadu spojení nalezneme velké množství informací o automatické změně filtrů bezpečnostního profilu na Intrusion*

Prevention Systému. Náznak možného problému - IPS blokuje provoz OSPF. Pokusně přepneme IPS do transparentního režimu, kdy systém neprovádí blokování provozu. Z logů pro IPS zjistíme, že se omylem na IPS distribuoval profil pro IDS režim. Tato distribuce byla vyvolána chybou v popisu profilů. Po vypojení IPS se sestaví OSPF spojení. Další analýzou logů z IPS zjistíme, že byl od provedení konfigurační změny na IPS v činnosti filtr, který blokuje přenos paketů, jejichž TTL = 1. Počet zásahů daného filtru po celou dobu narůstal. Síťovému technikovi je jasné, že mezi pakety, jejichž TTL je rovno jedné jsou i pakety směrovacího protokolu a jejich zablokováním se rozpadly směrovací tabulky. Z Audit logů zjistíme, že kolega z bezpečnostního oddělení před třemi dny chybně přejmenoval bezpečnostní profil v IPS, který se posléze automaticky distribuoval. Příčina byla nalezena, chyba byla odstraněna. Poučení pro odstranění podobného problému v budoucnosti: zrušit plně automatické distribuce bezpečnostních profilů a provádět je pouze asistovaně – Tj. systém vyzve k distribuci profilu, ale administrátor musí distribuci vždy aktivně odsouhlasit.

Screenshoty z LOGmanageru:

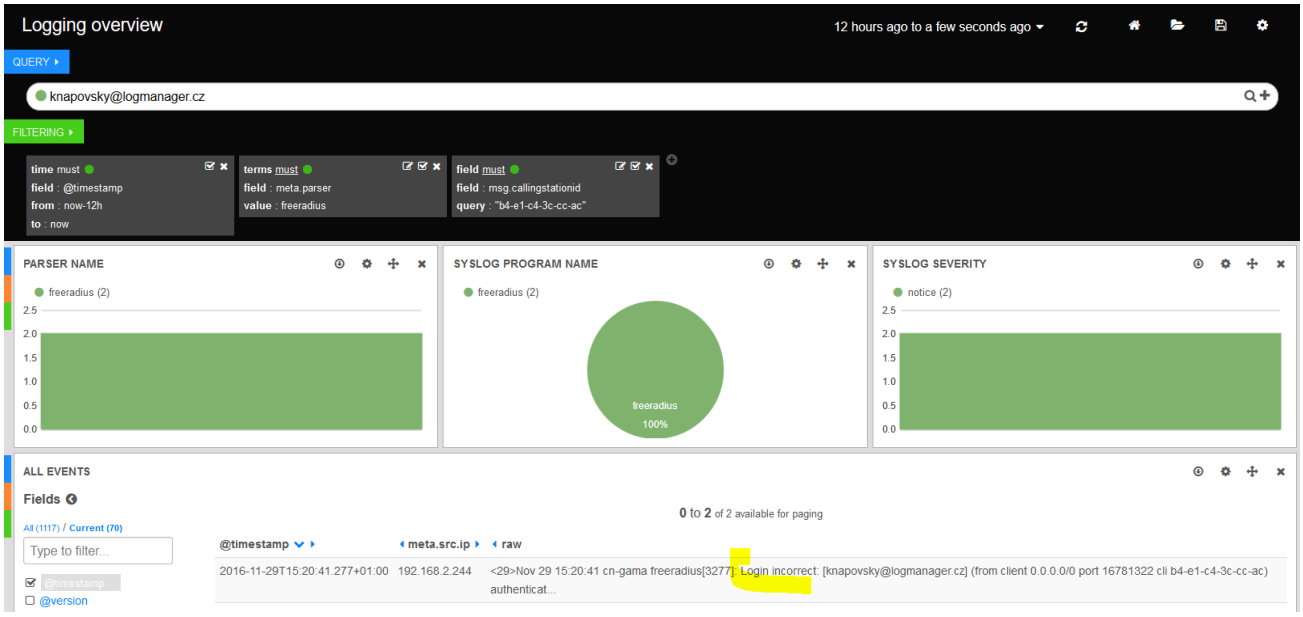


Změna množství blokovaných eventů v čase naznačuje, že se něco změnilo. Výběrem časového období za horizont počátku kritického IT incidentu vidíme nárůst TTL=1



Sjednocení formátu logů a jejich centralizace. Dalším problémem souvisejícím s doporučením nasazení centralizovaného systému je distribuce logů v zařízeních a systémech, rozdílná retence a jazyk logu. Každé zařízení si logy řeší plus minus samostatně, zapisuje je ve vlastním jazyce a má rozdílnou velikost paměti pro ukládání logů a tím i rozdílnou retenci (časové období zpětně), po kterou logy udrží. Pokud něco hledáte z provozních důvodů, musíte prohledat logy v různých zařízeních, pochopit, kde v nich hledané informace naleznete v každém jednotlivém záznamu a prohledávat a prohledávat. Centralizovaný systém typu LOGmanager Vám logy ze všech zařízení sesbírá a uloží na jedno místo. Dále je díky zabudované normalizaci událostí přeloží do jednotného jazyka, kterému snadno rozumíte a všechny pole záznamů indexuje pro rychlé vyhledávání. Když posléze řešíte nějaký provozní problém, tak se na jednom místě můžete podívat současně do logů z přepínačů, firewallu, MS Active Directory i aplikace, na kterou se přístup nedaří a odpověď se hledá rychle a efektivně.

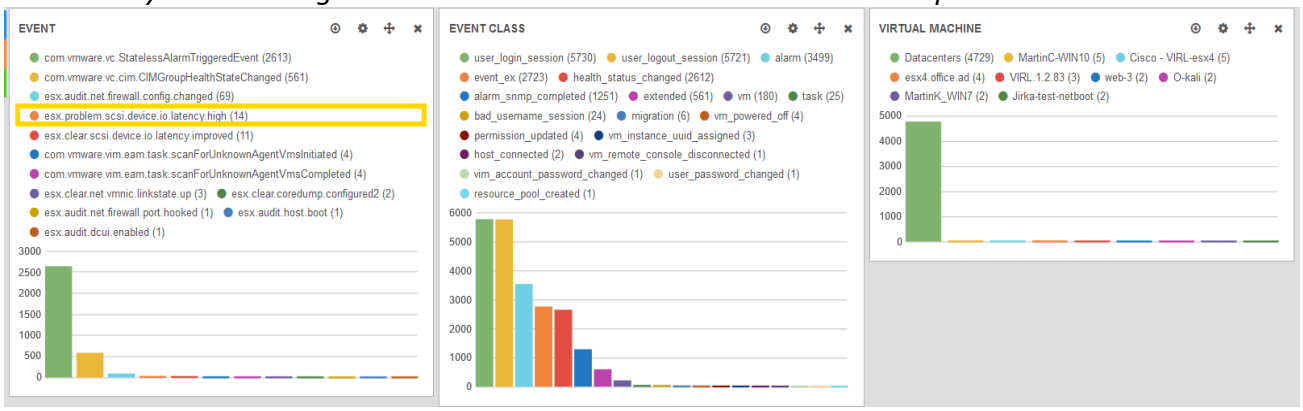
Příklad použití LOGmanageru pro analýzu provozního problému s využitím centralizace logů. *Jednomu ze zaměstnanců se nedaří přihlásit z notebooku k bezdrátové síti s 802.1X ověřováním. Vstupní informace – Uživatelské jméno z Active Directory nebo MAC adresa bezdrátové síťové karty daného notebooku. Naleznu informaci o opakovaném neúspěšném přihlašování do sítě pro konkrétního uživatele nebo MAC adresu jeho počítače. Podívám se do Active Directory, uživatel však nemá zablokovaný účet. Podívám se do logů RADIUS serveru (Network Policy Serveru v AD nebo Freeradiusu) a naleznu, že certifikátu nebo heslu, kterým se počítač v 802.1X procesu přihlašuje vypršela platnost.*



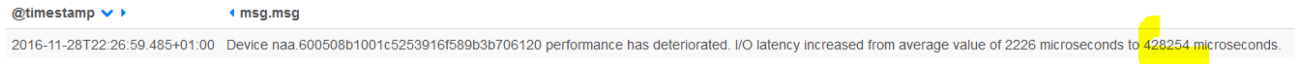
Rychlá analýza díky centralizaci logů. Díky centralizaci logů v LOGmanageru se technikovi IT otevírá možnost k rychlé analýze informací z mnoha zdrojů bez nutnosti mít ke všem systémům administrátorský přístup. Uložené logy nelze v LOGmanageru žádným způsobem smazat ani modifikovat. Proto lze technickému personálu bez administrátorských práv umožnit prohlížet logy většiny provozních systémů bez nutnosti udělit jim práva přístupu k systémům samotným. V rámci svojí práce poté mohou analyzovat běžné provozní problémy a komunikovat požadavek na jejich vyřešení dál v hierarchii IT.

Příklad použití LOGmanageru technikem bez přístupových práv k aplikacím a virtualizaci. *Uživatelé si stěžují, že jejich kritická aplikace za posledních 30 minut zásadně prodloužila odezvu a některé úlohy se dokončují až po 1minutovém čekání. Běžně však daná aplikace odpovídá v řádu jedné sekundy. Pohledem v LOGmanageru na záznamy z databázového serveru není nalezen kritický log. Pohledem na log z VMware vCenter jsou vidět významné incidenty popsané jako „IO Latency Increase" z 2ms na 428ms. Pohledem na log diskového subsystému NFS lze dohledat, že došlo k výpadku disku 0:8 v diskovém poli a příslušné pole zahájilo opravu za využití spare disku. Zpoždění na diskovém subsystému zapříčinilo zhoršení odpovědi aplikace, která s tímto NFS pracuje. Technik zaznamená závadu a předá ji správci NFS k okamžitému řešení. Pro danou analýzu nemusel mít přístupová práva k vlastní virtualizaci ani k NFS, přesto problém rychle lokalizoval.*

Screenshoty z LOGmanageru: Pohled na souhrn eventů z Virtualizace za posledních 6 hodin:



Detail eventu IO Latency High:



Bezpečnostní oblast

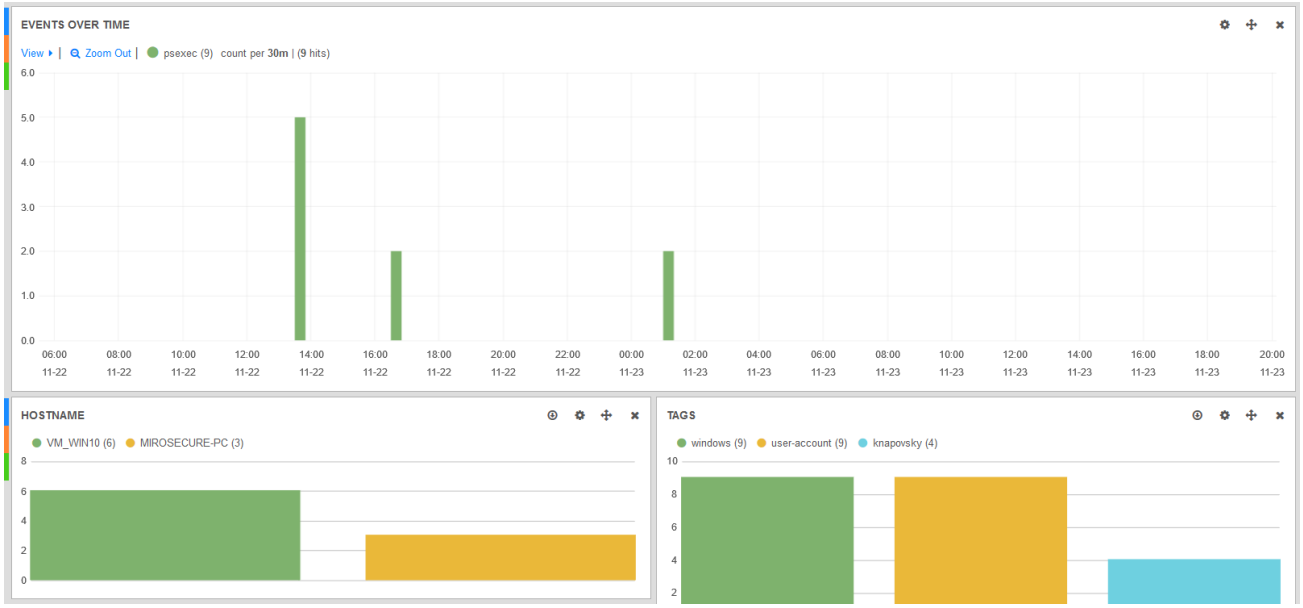
V bezpečnostní oblasti se jedná hlavně o **nezpochybnitelnost záznamů**, možnosti proaktivně hledat potencionální bezpečnostní rizika, ladit konfigurace a sledovat provedené změny. Když jednou LOGmanager nějaké záznamy uloží, nelze je vymazat ani modifikovat. Organizace řeší bezpečnostní problém, útočník ale obvykle informace o svojí činnosti na systémech a zařízeních, ke kterým získal neautorizovaný přístup maže. Proto může být velmi složité obnovit informace o jeho činnosti a poskytnout tyto informace pro důkladné vyšetření incidentu.

Důležitým předpokladem pro efektivní analýzu logů nejen v bezpečnostní oblasti je samozřejmě vhodná konfigurace zdrojových systémů. I s tím Vám LOGmanager pomůže. Součástí dokumentace jsou podrobné návody, jak zdroje logů nastavit tak, aby měli požadovaný obsah i formát pro zpracování a hlavně nesly informace, které k analýze budete potřebovat. Pro příklad níže například potřebuje zapnout v Microsoft AD Group Policy správným způsobem Advanced Audit pro spuštění procesů a vytvořit registy klíč, který monitoruje příkazy příkazové řádky. I to je součástí dokumentace.

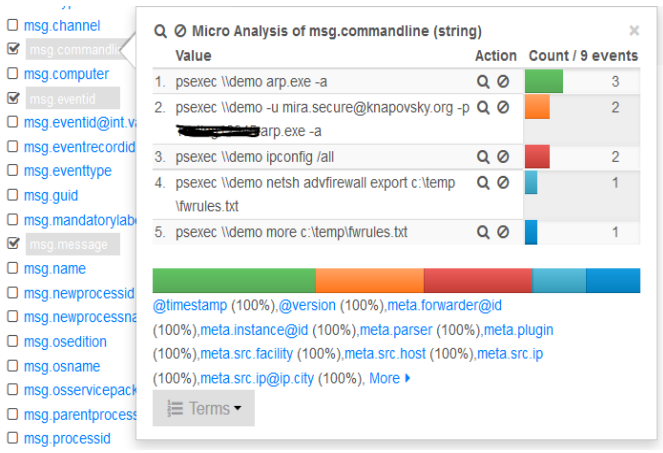
*Příklad z **dohledání příkazů příkazové řádky** na počítači, který hacker použil jako vstupní bod do sítě. Předpokladem je správně provedená distribuce LOGmanager komponentu WES (Windows Event Sender) do počítačů a serverů organizace a je dle doporučení správně nastaveno auditování. Windows systémy totiž zajímavé logy dávají až po vhodné konfiguraci, nikoliv defaultně. Potom se mohou v LOGmanageru nalézat logy o činnosti na každé stanici nejen ze 4 základních Windows logů (Application, Security, Setup a System), ale i z Application and Service Logs. Příklad takového extended logu s pokusem o přístup k administrátorskému zdroji:*

The SMB client failed to connect to the share.
Error: {Access Denied}
A process has requested access to an object, but has not been granted those access rights.
Path: \198.19.254.146\ADMIN$

*Logy lze samozřejmě filtrovat, takže jde zamezit zahlcení logy bez provozního nebo bezpečnostního kontextu. V tomto příkladu bezpečnostního technika však zajímají příkazy z příkazové řádky, které spouštěly vzdálený proces. Často užívaným nástrojem nejen administrátory, ale i hackery je třeba **PsExec** - a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tool. Příklad zobrazuje nalezení spuštění psexec v příkazové řádce včetně stanic, na kterých byl příkaz použit.*



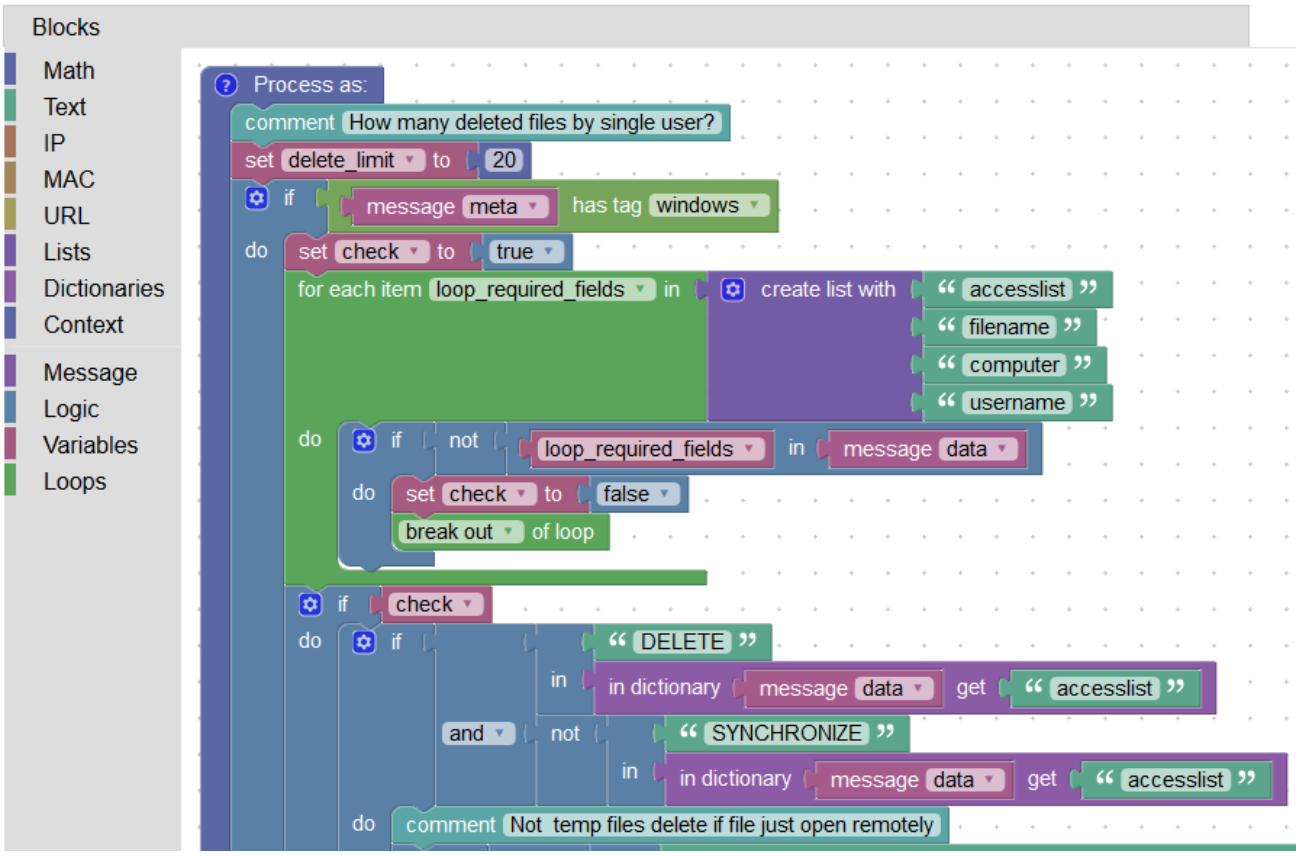
Pokud je třeba si nechat dynamicky zobrazit nejčastější příkazy ve spojení s psexec.exe, stačí si v menu polí vybrat pole msg.commandline a LOGmanager vypíše příkazy poslané v daném kontextu. Samozřejmě lze na volání příkazu na stanicích vytvořit i alert, aby administrátor bezpečnosti byl okamžitě informován, pokud někdo používá některý z podezřelých příkazů jako například v tabulce níže.



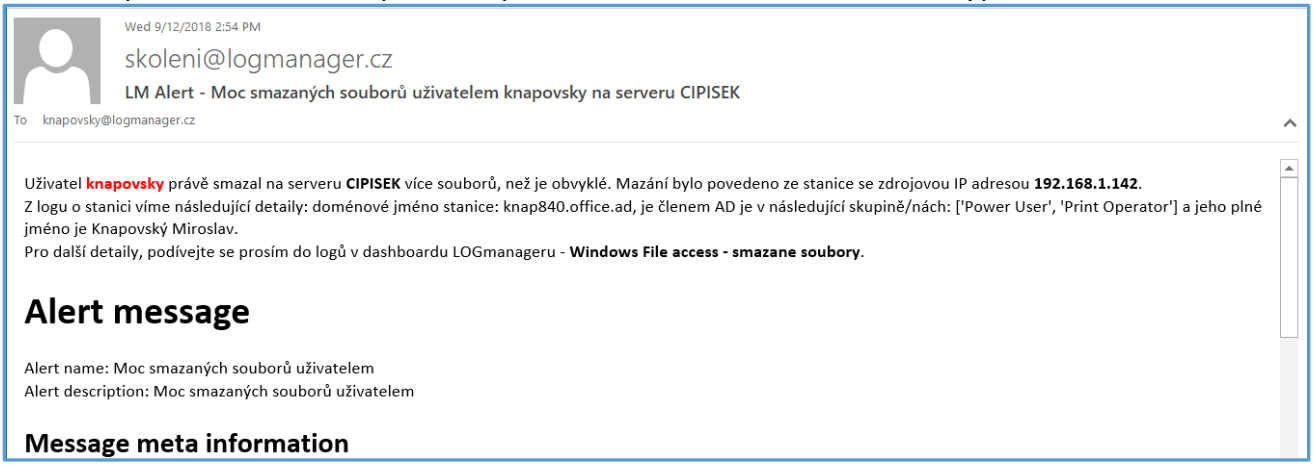
***Další zajímavé příkazy volané z příkazové řádky ke sledování**: arp.exe; at.exe; bcdedit.exe; bcp.exe; chcp.exe; cscript.exe; csvde; dsquery.exe; ipconfig.exe; mimikatz.exe; nbtstat.exe; nc.exe; netcat.exe; netstat.exe; nmap; nslookup.exe; netsh; OSQL.exe; powershell.exe; powercat.ps1; psexecsvc.exe; psLoggedOn.exe; procdump.exe; qprocess.exe; query.exe; rar.exe; reg.exe; route.exe; runas.exe; rundll32; schtasks.exe; sethc.exe; sqlcmd.exe; sc.exe; ssh.exe; sysprep.exe; systeminfo.exe; net.exe; reg.exe; tasklist.exe; tracert.exe; vssadmin.exe; whoami.exe; wscript.exe; wmic.exe*

Proaktivnost – pokud správně nastavíte v LOGmanageru alerty, případně korelace, bude Vás systém automaticky informovat o incidentech, které na základě více sledovaných parametrů zjistí a organizace může rychle reagovat na vzniklý problém. LOGmanager na jednom místě schraňuje informace o prováděných operacích v jednotlivých systémech, takže můžete snadno identifikovat, kdo změny provedl a s jakým výsledkem. Dále můžete sledovat například neúspěšné pokusy o přihlášení k systémům, které nesou citlivá data, pokusech o testování bezpečnostních pravidel ve vnitřní části sítě a podobně.

Příklad z využití LOGmanager pokročilých alertů – upozornění ***na nadlimitní množství smazaných souborů ze serveru.*** *Jako operátor bezpečnosti chcete být informován, že vám někdo (kdokoliv) hromadně promazává soubory na souborovém serveru s důležitými daty. Nastavení Alertu s thresholdem se provede s využitím zabudovaného vzoru pouhou modifikací, o který konkrétní server se jedná, a nastavením počtu smazaných souborů, které mají vyvolat automatické upozornění.*



Nastavení Alertu lze snadno otestovat a upravit si formátování upozornění dle vlastních představ. Příchozí upozornění si může operátor upravit k obrazu svému, a tak může vypadat třeba následně:


Wed 9/12/2018 2:54 PM

skoleni@logmanager.cz

LM Alert - Moc smazaných souborů uživatelem knapovsky na serveru CIPISEK

To knapovsky@logmanager.cz

Uživatel **knapovsky** právě smazal na serveru **CIPISEK** více souborů, než je obvyklé. Mazání bylo povedeno ze stanice se zdrojovou IP adresou **192.168.1.142**.
Z logu o stanici víme následující detaily: doménové jméno stanice: knap840.office.ad, je členem AD je v následující skupině/nách: ['Power User', 'Print Operator'] a jeho plné jméno je Knapovský Miroslav.
Pro další detaily, podívejte se prosím do logů v dashboardu LOGmanageru - **Windows File access - smazane soubory**.

Alert message

Alert name: Moc smazaných souborů uživatelem
Alert description: Moc smazaných souborů uživatelem

Message meta information

Dále lze alerty zachycené logy snadno přeposlat na nadřazený SIEM server prostřednictvím syslogu.

Soulad s regulacemi a zákony

V oblasti **souladu s regulacemi** je výzev hned několik. Pokud se jedná o organizaci, která spadá pod státní kritickou infrastrukturu, musí organizace schraňovat a analyzovat záznamy o činnosti jednotlivých zákonem definovaných činností, systémů a prostředků. Ale protože těchto organizací není mnoho, jedná se spíše o soulad s novou regulací evropské unie – GDPR. General Data Protection Regulation je povinná pro všechny organizace, které ročně zpracovávají více než 5000 záznamů o subjektech v evropské unii. A pod záznamy se rozumí jakékoliv osobně identifikovatelné údaje, včetně údajů o klientech, zaměstnancích i právních subjektech. Je to prakticky cokoliv, co identifikuje daný subjekt: jména, adresy, email adresy, rodná čísla, čísla osobních průkazů, ale třeba i IP adresy, které daný subjekt používá a jsou v záznamech organizace. GDPR požaduje, aby měly organizace funkční procesy pro poskytnutí detailní dokumentace bezpečnostního problému a musí být schopné tyto informace poskytnout pro audit i možné vyšetřování. GDPR se vyjadřuje velmi obecně a vyžaduje vytvoření nových politik, vnitrofiremních rolí a vztažených povinností.

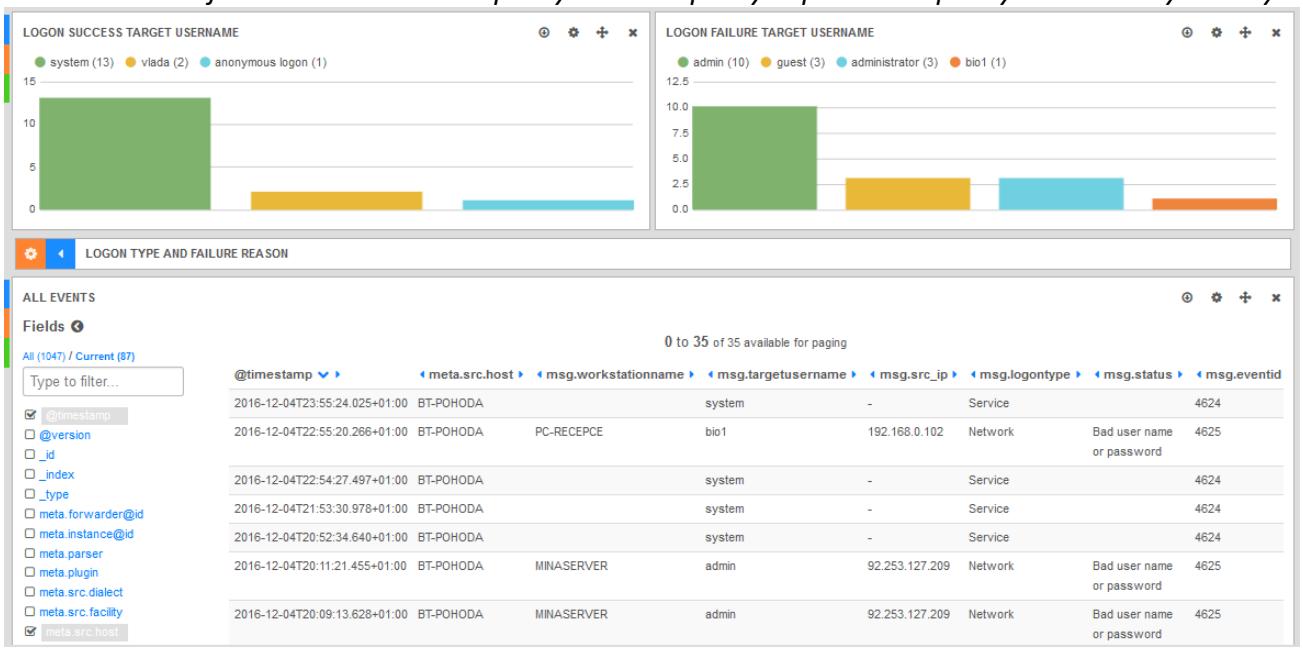
Audit/Reporty - pokud organizace prochází auditem bezpečnosti, je systém, který dokáže vygenerovat reporty dle požadavků auditora nutností. LOGmanager umožňuje generovat reporty nejen v grafické podobě, ale i v CSV se strukturou, kterou si auditor pro svoji analýzu definuje. Lze vybrat libovolné pole z databáze, zahrnout je do reportu a vyexportovat klidně soubor s desítkami tisíc řádků. Dále LOGmanager obsahuje možnost přistupovat prostřednictvím REST-API přímo k databázi a formátovat požadavky proti databázi vlastním reportovacím nástrojem.

Příklad z praxe: LOGmanager je řešení, které monitoruje a nezpochybnitelně dokládá mimo jiné přístup k systémům s personálními daty a generuje alerty, když systémy detekují pokusy o neautorizovaný přístup. V případě průniku zajistí plný set logů z těchto systémů, které lze doložit vyšetřovatelům bezpečnostního incidentu i národnímu dohledovému orgánu. Vyšetřovatel chce všechny informace o přístupu k systému s kritickými daty v textovém formátu a požaduje pole přesného času incidentu, uživatelského jména, zda byl přístup povolen či odepřen a jaká byla zdrojová adresa systému, ze kterého byl pokus vzdáleného přístupu zaznamenán.

Screenshot exportu vybraných dat v CSV formátu na základě požadavku auditora:

	A	B	C	D	E	F	G	H
1	@timestamp	meta.src.host	msg.workstationnar	msg.targetusername	msg.event	msg.logontype	msg.status	msg.src_ip
2	2016-11-16T23:34:21.157+00:00	BT-POHODA		dwm-4	4624	Interactive		-
3	2016-11-16T23:34:21.124+00:00	BT-POHODA	STOUPICEK-G770	vlada	4624	Network		-
4	2016-11-17T15:38:51.673+00:00	BT-POHODA	BT-POHODA	vlada	4624	RemoteInteractive		46.135.xxx.xxx
5	2016-11-17T00:09:24.986+00:00	BT-POHODA	BT-POHODA	vlada	4624	RemoteInteractive		89.239.xxx.xxx
6	2016-11-17T00:08:32.951+00:00	BT-POHODA	STOUPICEK-G770	vlada	4624	Network		-
7	2016-11-18T16:10:14.634+00:00	BT-POHODA	CLOUD	administrator	4625	Network	Bad user name c	117.21.220.247
8	2016-11-18T16:10:12.524+00:00	BT-POHODA	CLOUD	administrator	4625	Network	Bad user name c	117.21.220.247
9	2016-11-18T22:23:13.513+00:00	BT-POHODA	13BC8FD6A1CC4F2	administrator	4625	Network	Bad user name c	222.239.10.168
10	2016-11-18T10:09:31.075+00:00	BT-POHODA	SILEQRDS01	guest	4625	Network	Bad user name c	210.215.71.90
11	2016-11-18T10:09:44.300+00:00	BT-POHODA	SILEQRDS01	admin	4625	Network	Bad user name c	210.215.71.90
12	2016-11-18T10:08:54.406+00:00	BT-POHODA	SILEQRDS01	anonymous logon	4624	Network		210.215.71.90
13	2016-11-18T10:08:56.442+00:00	BT-POHODA	SILEQRDS01	administrator	4625	Network	Bad user name c	210.215.71.90
14	2016-11-18T10:09:19.833+00:00	BT-POHODA	SILEQRDS01	guest	4625	Network	Bad user name c	210.215.71.90

Screenshot zdrojového dashboardu úspěšných a neúspěšných přihlášení pro systém s citlivými daty:



Časté otázky

Co za logy a události je třeba sbírat a sledovat? Odpověď je skryta v porozumění hlavního účelu sběru strojových dat. Obecně platí, že sbírat by se mělo vše, co má hodnotu pro účel sběru. Hlavní účely jsou tři – provozní, bezpečnostní a zákonné. Tomu je potřeba přizpůsobit nastavení zdrojových systémů. Jedná se průběžnou činnost, protože nové systémy se přidávají a staré modifikují nebo odebírají. Je třeba trvale sledovat změny v IT strukturách a do managementu změn zařadit položku Logování a Audit. Co do objemu dat, vždy je lépe sbírat co nejvíce a nejpodrobnější data. Filtrovat nerelevantní data LOGmanagerem je snadné. Příměrem: v kupě sena vhodným nástrojem jehlu najdete, ale nenajdete ji v hromádce sena, kam jehla nebyla od počátku vložena.

Jak dlouho strojová data schraňovat? Zde je odpověď snadná. LOGmanager poskytuje více než dostatečnou kapacitu rychlého diskového prostoru pro databázi, takže při sběru například 250GB strojových dat denně je retence dat na nejvyšším modelu LOGmanageru déle než jeden rok. To jde za požadavek většiny regulací i provozních důvodů. Pokud je diskový prostor LOGmanageru naplněn, administrátor systému dostane notifikaci, že systém smaže nejstarší den záznamů, aby uvolnil místo pro nové záznamy. Ukládání nových a konzistence starších dat není během této operace narušena. Nestačí? LOGmanager umožňuje sbíraná data automaticky zálohovat na externí SMB server.

Kolik mne dané řešení bude stát? LOGmanager je systém bez skrytých nákladů. Systém nepoužívá licence na zařízení ani na množství logů. Cena je za řešení včetně optimalizovaného hardware, dle typu krytého 3 nebo 5letou výměnou od výrobce. Software upgrade a technická podpora na první rok je v ceně. Prodloužení podpory a SW upgrade je stanoveno jako 15% z prodejní ceny produktu.