

Po kliknutí na položku menu CM IT Monitoring -> Event server -> Udalosti zo zberov sa vám zobrazí zoznam, obsahujúci udalosti nachádzajúce sa na serveri, zoradené od najnovších po najstaršie.

Vo vrchnej časti zobrazenia je možné filtrovať zobrazené udalosti na základe:

- názvu spoločnosti,
- názvu zberu,
- názvu počítača (CMID aj názov počítača),
- periódy výskytu,
- užívateľa

V predvolenom zobrazení sú uvedené informácie (stĺpce):

- spoločnosť,
- počítač (CMID),
- názov zberu,
- typ udalosti,
- dátum a čas výskytu,
- skupina do ktorej daná udalosť patrí,
- stav udalosti (Potvrdenie),
- EventID udalosti,
- meno logu,
- popis udalosti (v skrátenom a zjednodušenom tvare),
- poznámka k udalosti.

Stĺpce spoločnosť, počítač a názov zberu majú fixnú pozíciu a nedajú sa odstrániť. Pre lepšiu prehľadnosť sú sa však dajú skryť kliknutím na ikonu šípky, nachádzajúcu sa v ľavej časti zobrazenia.

CD	ESK		Adm	nin pórus	OM I	T monitoring	• •	005K	ſ	Vichry	filter	Dialog	a pre		Sinversity. Evening probled $$ Hermonic fibrition: BA Sentrop \sim	
10	Event server C	E	ver	nts from	1 collect	tor tasks				-		stips				
-	17 Jechenikové načitanie 15 Udalesti za zberov 🔕	0	Company Collector Task			Company Baar Period Los 2 days # 900			· Nop Not	NAME OF A					Filter v Contine v	
	Silveni Italidiy	Π	•	Company	0840	Collector Task	Туря Т	Data Timo	Graup T	Event ID T	Confirmatio	n Log Name	Searce	Tank	Description	
244 Deletateria	Poheticovado providiá	П	0	-		Allenjoine	to have a dear	20.04.2010.12.32.33	Loge	21	al mice (a	Manual Vincous Team	IRocket restore from		Lugget-ol. 384/www.10-40.28	
i			0	NPL 44	DV/DVDC	1894, 1894	Repairy	20-04-2018 11-40-5	index in	•	ainionia	HER LOCAL MICHINE	Registry		Multiple wirelative pairy key for VILVEP 10.22.00, 10.22.001 (JICEE2000.3275.4.001.0730.7000.0716.00	
Manaforda) attention	Schová stípce		0	9095-64	51/180040	Zakaduroatko	Critical	2014/2015 07:52:0	Coor .	-	01210219	Monanth Vindows-Olagne	Minoret Vindows-Bager		Soften maintenance detected to see requiring your attention. A multication uses sent to the Action Center,	
12	Company, CM-ID a	П			-	2000,0000	CHINA	2010/2010 07:02:0	and a	-	divide (a	Monanth Wedner-Chapto	Mused Andres Bayes		System manhearce detached souse requiring your attention A walfordism und sent to the Action Center.	
Denterver	Collector Task	Н	0	are sea		Zalial_yestic	Critical	20-04-2018-07-82-11	i line	100	ainionia	Manual Vision Dage	Manual Vision Days		System matchesismen detected in cars, requiring your attention. It multitudion cruss cerei to the Taction Device	
		1	0	9CP6-11	51/1700000		Orient	2014/2015 00:42:45	Ceor .	-	01210219	Monanth Vindows-Oligne	Microsoft Windows-Blager		Some mathematic detected is see requiring your attention, λ with a time see sent to the λ close Darker .	
			0	9CP5-61	-	Aprel	CHINA	2010/2010 06:42:11	a marcine a	100	divitavia	Monand Wedner-Claps	Mixed Andres Bayes		System manhesing detailed asses requiring your attention. A sufficiency use send to the Action Defair	
			0	RPI-14	BANKCOMO		Critical	20-04-2011-04-02-11	i line	100	al-loria	Mercard, Vinters, Diagra	Monoral Vision Dage	Mankers with splaces price	$\label{eq:states} System We down we specify Transit accelerate : TMMM are indicegoalisation : being Tax inside to (UTC) : TMM and the transition of the tr$	
			8	area.	51/17/20000	ALexen	Oritical	2014/2015 00:02:0	Ceor .	***	01210219	Monanth Vindows-Oligne	Microsoft Windows-Blager	Nonio svanie vskom pris	Soutien Websen as specify Transic providence: (1946) we inDegradation: Note Trailections (UTO) : 1014	
					-		to have a disc	20.04.2010.00.00.00	Powerstee	+000	01+10+18	security.	INCOME PRODUCTION	Security State Change	Medices & starting up. The events logged when C2H22 2012 starts and the auditing auto-presents indicated	

Obrázok: Popis základného zobrazenia

Ak chcete zobraziť detailné informácie udalosti, kliknite na zvolený riadok. Otvorí sa vám dialógové okno v ktorom dodatočne vidíte (ak sú dostupné):

- rolovací zoznam pre zadanie stavu potvrdenia,
- užívateľa ktorý zadal posledný stav potvrdenia,
- údaj o dátume a čase poslednej zmeny stavu potvrdenia,
- zdroj z ktorého pochádza udalosť (Source),
- úlohu, ktorá vytvorila udalosť,
- úroveň výstrahy (level),
- operačný kód,



Správa načítaných udalostí

Zverejnené na Customer Monitor (https://customermonitor.sk)

- kľúčové slová,
- užívateľské meno,
- názov počítača,
- doménu,
- číslo záznamu,
- popis udalosti v zjednodušenej podobe (a prípadne príslušné binárne dáta),
- pole pre zadanie poznámky,
- originálne znenie udalosti (generované operačným systémom),
- XML znenie udalosti (generované operačným systémom).

Confirmation Type:	* Sa	Description:	XML:	
Note:	Sa	Account SEPSASIsandrah Logon ID: 0x5C9DF01 Object Name: C:Usersisandrah/uppData/Local/MicrosoffCredentals Process Name:	<event subjectusersid"="" xmins="http://schemas.microsoft.com/win/2004/08/events/event>
<System></th></tr><tr><th>Computer Code: SVY</th><th>/SV003</th><th>C:Windows/System32/Isass.exe Access: ReadData (or ListDirectory)</th><th><Provider Name=Microsoft-Windows-Security-Auditing
Guide/\S449625-543-4994-A5BA-3E3B0328C30D)/>
<EventD>4663<(EventD></th></tr><tr><th>Company Name: SEPS</th><th>S, a.s.</th><th>Binary Deta:</th><th> Variation-U Variatio</th></tr><tr><th>Collector Task: Collec</th><th>ict_important</th><th>Original Description:</th><th colspan=4> Cpcode=u=<0pcode= Keywords>0x80200000000000000000000000 Keywords> TimeCreated SystemTime=2015-04-20106:58:29.9800301002/> EventPacontID::56123864:EventPacontID:: </th></tr><tr><th>Log Name: Secu</th><th>urity</th><th>An attempt was made to access an object.</th><th><Correlation/> <Evecution ProcessID=4* ThreadID=76/> <Channel>Secutive/Channel></th></tr><tr><th>Pohyb med</th><th>zi
Date Time: 20.04.2015.06.58:</th><th>Subject
Security ID: 8-1-5-21-2711929835-549276958-3169794103-
1660</th><th><Computer-PSWS214021.sepsas.sk </Computer>
<Sacurity/~
</Sacurity/~</th></tr><tr><th>Event ID: 4663</th><th>3 Task: File System</th><th>Account Name: sandrah
Account Domain: SEPSAS
Logon ID: 0x5c9dt01</th><th>«EventData»
«Data Name=">S-1-5-21-2711929835-549276958- 3169794103-1660</event>	
Level: Infor	mation Oper. Code: 0	Object Object Server: Security Object Type: File	«Data Name=SubjectUserName>sandrah-(Data» «Data Name=SubjectDomainName>8EP8AS-(Data» «Data Name=SubjectLogend>0x5c9d01-(Data» «Data Name='ObjectServer>Security-(Data>)	
Type: Infor	mation Key Words: Audit Success	C:Usersisandrah/AppData/Local/Microsoft/Credentials Handle ID: 0x15e4	«Data Name+'ObjectType'>File <data Name='ObjectName'>C1UsersisandrahiAppDataiLocal/MicrosoftiC Name='ObjectName'>C1UsersisandrahiAppDataiLocal/MicrosoftiC</data 	
User Name:	Computer: PSWS214021.seps	s.sk: Process Information: Process ID: 0x1e8 Process Name: C:Windows/System379sass ave	als-(Data» -Data Name="Handleid"-0x15e4-(Data» -Data Name="AccessList=%%4416	
Domain:	Record N.: 66123864	Access Request Information: Accesses: ReadData (or ListDirectory) Access Mask: 0r1	<data name="AccessMark/">bc1 Data Name=ProcessMark/>bc1 Abata Name=ProcessMare/>C.Windows/System32%ass.exe Data Name=ProcessName/>C.Windows/System32%ass.exe</data>	

Obrázok: Detail udalosti

V detaile udalosti je taktiež možný prechod na ďalšiu alebo predchádzajúcu udalosť a to pomocou smerových šípok (▲ a ▼) nachádzajúcich sa v ľavej časti dialógového okna. Date: 9.6.2015