

Prostredníctvom CM môžete lepšie zaistiť vašu počítačovú sieť, prípadne zistiť informácie súvisiace s bezpečnosťou nekolidujúce s ochranou informácií. Ponúkame vám zopár tipov na využitie tohto veľmi komplexného nástroja.

Výpis s historickými údajmi za posledných 6 mesiacov, aký typ používateľa sa prihlasuje

Detekcia spusteného procesu s identitou neoprávneného administrátora

Monitorované sieťové prenosy mimo LAN s určením čísla portov a cieľovej IP adresy

Zoznam procesov s určením vlastníka, ktoré sú spustené na počítači (aktuálny stav)

Spustenie programu vyžadujúceho admin.práva u používateľa, ktorý má odopreté admin.práva

## Výpis s historickými údajmi za posledných 6 mesiacov, aký typ používateľa sa prihlasuje

Otvorte si v CM CM IT monitoring -> Zóny -> Registračné info. K danému počítaču si otvorte históri a uvidíte tam, kto sa kedy prihlásil s akými oprávneniami. Okrem toho tu vidíte aj zapamätané, kto mal daný počítač v používaní podľa CM registrácie, aké bolo sieťové meno počítača v minulosti. Zaujímavé informácie, ak potrebujete sledovať pohyb počítača po firme (tieto údaje budú zoskupené v CMDB)

CD	ESK	Admin z	óna CM IT mo	nitoring C	DESK		Slover	rsky Kredit Manual	Operátor: Meno Operátora 🗸					
<u></u>	Zobrazenia C	🚦 Zói	ny						? 9,					
Osfilaeni I	😴 Počilače 7. Online informácie	Registračné k	Spoločno     Spoločno     Operátor     Op	**	Počitać & Umiestnenie Zoradiť podľa Ol	Použivateľ D • Zoradiť ak	Vzostupe ·	Hatet OC						
Upscomente	Walches	-	Os.		Zahmát ručne	zadané počítače 📋 Len o	nine počitače							
	🚗 Internet bandwidth monitor	História zón	História zóny: Registračné Info											
(Q)	🔿 Zùny	Zobrazit	0.0 02.03.2011	00:00 do	Vytvorené	ne politeli 🔹 Ze	braziť							
Zobrazenia	😳 Zmeny na počítači	Počítač NOR	INB13 - 7068 - Daniel - 1	el Jiham s.r.o. (PREMIUM licencia)										
- Ch	😅 Foto dokumentácia	Langeda -	weeni											
Aplication	SCMDB Dashboard	23 Seb 3813 0 Dec 3013 0 Jan 2012												
		Parameter	13/23/21	13:25:47	9. Jan 2012 08:30:15	25. May 2011 17:03:42	25. May 2011 16:43:35	12. May 2011 18:36:56	12. May 2011 18:36:11					
		Network Name	7069	7068	7068	7068	7069	7068	7069					
syntemove		User	Daniel	Daniel	Duriel	Daniel	Daniel	Duniel	Daniel					
i Nauderské		Computer network name	7058	7058	ME13706A	NB13706A	NB13T06A	NB13706A	NB13706A					
informácia		Network	Domain: nem.local	Domain: nam.local	Domain nam.local	Domain nem.local	Domain: nam.local	Domain: nem.local	Domain: nam.local					
		User	Daniel	Daniel	Patrik	Zuzano	Zuzann	Zuzann	Zuzana					
		Current login	NAMBAR	NAMadministrator	NAMES	NAMMedministrator	NAMES	NAMadministrator	NAMING					
		User type	User	Admin	Admin	Admin	Admin	Admin	User					
		Email	hat@firma.sk	hot@firma.sk	in@fma.sk	tube@tmask	truba@firma.sk	tube@fmask	truba@trma.sk					
		Location	709C	7060	8096	706e, P0608023	706a, P0609023	706e, P0608023	706a, P0608023					
		Internet	Permanent	Permanent	Permanent	Permanent	Permanent	Permanent	Permanent					

Obrázok: História počítača v Zóne Registračné info ukazaujúca okrem iného, aký používateľ bol s akými oprávneniami prihlásený.

#### Detekcia spusteného procesu s identitou neoprávneného administrátora

Vyššie popísaný prípad nezachytí, ak niekto na počítači spustí proces spôsobom Run As. Na tento prípad má CM prichystanú Watches podmienku Unauthorized Admin Process. Táto podmienka sleduje každých 30sekúnd, či nie je spustený akýkoľvek proces pod používateľom s administrátorskými oprávneniami mimo dovolených administraátorov. Efektívne aj voči prelomeniu účtu lokálneho administrátora. S touto podmienkou ustrážite spočítače, aby vám na ne šikovní



X

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

## používatelia nepriinštalovali nebezbečné softvéry.

Ak ste s Watchmi ešte nepracovali, prečítate si <u>Úvod do nastavenia monitoringu</u> [1].

#### Condition Definition

Filter	Unauthorized Admin Process
Ping Packet Loss         SMTP         POP3         HTTP, HTTPS         HTTP, HTTPS Response Time         Transfer Speed         Transfer speed of FTP         SNMP         Environment Monitoring (snmp)         Environment Monitoring (http)         E-Mail Loop Test	Running         No process of not authorized administrator         Authorized Administrators         Note: system accounts (e.g. SYSTEM) are automatically included into         "Authorized Administrators"         If you need more complex condition, see "Running User Process"         Value from this condition send to CM server         Image: Always
EventLog Events Count CHAT CHAT Variable CHAT Numeric Variable CHAT Vector Variable Service Status Loaded Device Driver Running Process Running User Process Unauthorized Admin Process Process Usage	Never Assess the state of watch
	OK Cancel

Obrázok: Watches podmienka (Condition) pre sledovanie spusteného procesu pod neautorizovaným administrátorom.

# Monitorované sieťové prenosy s určením čísla portov a cieľovej IP adresy

Zaujímavé výstupy viete získať cez internet bandwith monitor. Ak máte podozrenie, že niekam systematicky unikajú údaje nedovoleným spôsobom, môžete to nájsť cez <u>Internet Bandwith Monitor</u> [2]. Nájdete tu prehľady internetových prenosov z jednotlivých aplikácií, na cieľové IP adresy, rozdelenie na porty. Prehľad prostredníctvom ktorého určíte, či nejaký pracovník nerobí systematicky nekalú činnosť.

Ak by vás zaujímalo, že či niekto nepreniesol príliš veľa údajov, sú na to aj Watches podmienky (<u>Internet IP Trafic</u> [3], <u>Internet IP Transfered Data</u> [4]).

(v čase písania tohto príspevku sa spúšťa testovacia prevádzka už aj na všetkých 64bit systémoch okrem WIN8/ 2012. Doteraz boli podporené len 32bit systémy, takže záber tohto monitoringu je už dosť široký.)



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

ázov siete	P	ločítač & Umir									- opas	11 1011
			estrienie	P	'ouživateľ		Operátor	🔍 Hfadaj				
Octail po	icitada SA	GSVID.										. 0
Prenosová niz	chiost"	Prenesené	dáta Di	etaily preno	su PC O poi	itači						
					_		_				<b>15</b> Bh	
<b>1</b>		Od	01.02.2013	00.00.00	do 22.02.2	013 23:59:00					<b>1</b> 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
			SAGSV03	- Prenos di	it procesov roa	delený na TC	P porty a ost	stné protokoly, 01.02.2013 00:0	1:00 - 22.03	2013 23:59:00		
Proces	Total	Dowmoad	Upload	Port #: Do	wnioad/Upioad							
Manibor.ene	\$71,76 MB	833.08 MB	138.07 MB	110:	701.79 80	40.44 20	00:	100.02 HD / 70.07 HD	25:	1.54 80 / 19.54 80	222:	20.29
eventout.exe	357.59 MB	25.12 MB	212.47 MB	63353:	1.69 80	49.57 30	64412:	7.67 HB / 42.76 HB	90:	28.47 MB / 693.04 MB	62784:	2.56
""Unknown""	101.56 MB	59.79 MD	171.77 MD	80:	23.15 MB ;	79.03 38	1826:	4.31 HB / 13.18 HB	110:	1.73 38 / 15.18 38	1326:	5.02
MDist.eee	108.37 MB	80.94 MD	8.44158	80:	93.30 88	8.76 HB	4431	8.89 MB / 3.67 MB	2221	48.31 32 / 4.63 88		
re-8006- andoes-1588- Rousea	47.44.58	40.01 MB	880.85 13	00:	46.61 80	/ 050.05 10						
DescConstant	14.77 MD	14.08 MD	410.00 13	80:	14.33 88	/ 374.23 18	safp (	29.18 HB / 43.77 HB				
re-Bu08- aindoes-i688- Rausea	11.88 MB	11.65 MB	215.28 18	00:	11.65 80	/ 215.20 10						
utheck.eee	5.92 MB	5.70 MB	140.02 10	80:	8.78 88	/ 143.82 18						
Attalables.eee	2.73 M9	1.35 MB	2.37 MB	11438:	1.13 88	2.05 MB	80:	228.92 MB / 322.15 MB	110:	3,73 328 / 6.04 328	777:	132.00
Srefox.eee	2.58 MB	2.40148	80.12 83	80:	2.05 20	63.62 329	443:	140.07 10 / 26.00 10				
BIFLORE BIE	308.89 KB	308.87 109	27.42 18	00:	239.19 800	5.17 830	442:	69.47 HB / 22.25 HB				
AcroPi632 are	108.46 KB	95.24 83	4.22 KB	80:	92.56 KB /	3.24 KB	442:	2.69 HB / 1 001.00 B				
Adube-ATM.exe	98.76 KD	80.77 83	1.89 KD	80:	88.77 88	/ 1.99 KB						
upched.eee	92.12 K9	77.60 KB	4.50 K9	80:	77.63 828	4.80 88						
2120.000	20.34 K9	19.25 83	12.00 13	60:	18.25 800	18.99 328						
anotheols are	24.40 KB	11.32.08	11.18.19	00:	11.22 900	/ 10.10 300						
Jakasan .	1.00.00	1.12.00	7.52198									
	Processing Proces Andor ese whore ese wh	Process richlost Proces Total Anter ese 071 76 MB wrbot, ese 277 76 MB wrbot, ese 277 76 MB wrbot, ese 171 76 MB wrbot, ese 17	Process         Total         Prenesserie           Process         Total         Download           Ander-see         971.76 MB         620.66 MB           writer-see         977.96 MB         921.86 MB           writer-see         977.96 MB         921.86 MB           writer-see         977.96 MB         921.86 MB           writer-see         977.96 MB         921.84 MB           writer-see         977.96 MB         920.78 MB           writer-see         971.97 MB         92.94 MB           writer-see         193.37 MB         92.94 MB           writer-see         193.37 MB         92.94 MB           writer-see         193.37 MB         92.94 MB           writer-see         11.88 MB         11.46 MB           writer-see         2.92 MB         32.40 MB           writer-see         2.92 MB         32.40 MB           Writer-see         2.94 MB         2.94 MB           Writer-see         2.94 MB	Process richlost         Process dist         D           Image: State	Process         Total         Desking remo           Ander see         011 / 20 / 10         000 / 20 / 20 / 30         000 / 20 / 20 / 30           Ander see         011 / 20 / 10         000 / 20 / 20 / 30         000 / 20 / 20 / 30         000 / 20 / 20 / 30           Ander see         011 / 20 / 10         000 / 20 / 20 / 30         000 / 20 / 20 / 30         000 / 20 / 20 / 30         000 / 20 / 20 / 20 / 30           Ander see         011 / 20 / 10         000 / 20 / 20 / 20 / 20 / 20 / 20 / 20	Precess initialization         Precessed dist         Detaily areanosu PC         O poil           Col 01 02 2013 000000         Col 02 2022         Col 01 02 2013 000000         Col 02 2022           SAGSV03 - Precess dist processor area         Col 01 02 2013 000000         Col 02 2022           Proces         Total         Download         Upload         Port #: Download/Upload           Ander ese         011 /0 MB         603 68 MB         138.87 MB         1101:         701.79         20           Whotever         307 59 MB         251 240         21.47 MB         622 522:         1.69         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20         20	Precess righter         Preneseré dáis         Detair greeneu PC         O pointait           Image: State Sta	Precession initiation         Prenessend dists         Detaily preneou PC         O politikit           Image: Statistic constraints         Od (nr. 00.2013 00.000)         Image: Statistic constraints         Image: Statistic constatistic constraints         Image: Statistic c	Precesser initiate:         Precessed dist         Detaily precesse PC         O points i           Image: I	Precesse initiate:         Precesse dits         Detaly precess PC         O poliait           Image: Precesse dits         Od # 02.2013 00.00.00         Image: Precesse dits         Od 20.2013 23.99.00         Image: Precesse dits         Precesedits         Precesse dits         Precesse dits	Precesserii ritheter         Precesserii dits         Desky prenosu PC         O poiltă i           Image: I	Prenosme initiality         Prenosme data         Detaily prenosup PC         O pricitie           Image: Contract State S

Obrázok: Príklad výpisu prenesených dát cez internet jednotlivými aplikáciami

## Zoznam procesov s určením vlastníka, ktoré sú spustené na počítači

Bez akéhokoľvek nastavovania sa na počítači tvorí automaticky krátkodobá história (niekoľko dní dozadu každých 30sekúnd) dostupná cez C-MonitorConsole v Systémových informáciách. Ak potrebujete overiť, či bol spustený nejaký proces a s akými oprávneniami, tu ho nájdete. Procesy sa dajú aj dobre filtrovať, takže viete vidieť v akom intervale bol bol daný proces spustený. (História sa dá rozšíriť zväčšením archívu, ale má svoje limity, nakoľko toto nie je nástroj určený na detailné a dlhodobé sledovanie aktivity práce pracovníkov).

Viac informácií nájdete v článku Systémové info v rámci popisu C-MonitorConsole [5]



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

MonitorConsole						(color x
C-Monitor Tools Help		1	System	Info		G
👩 Settings	📖 🖬 🖻 👂 🖉	Filter	$\nabla$			
Scheduler	Date Time 😎	Description				
Watches	2013.02.22 15:10:30.951 2013.02.22 15:10:00.972 2013.02.22 15:00:30.952	System Info System Info				
C-Monitor Runtime Information's	2013.02.22 15.09.00.953	System Into				
Wating Tasks Running Tasks Watches State Watches Current Log C-Monitor Current Log System Runtine	2013.02.22 15.08.29.953 2013.02.22 15.07.59.945 2013.02.22 15.07.59.945 2013.02.22 15.07.59.950 2013.02.22 15.06.956 2013.02.22 15.06.09.956 2013.02.22 15.06.01.053 2013.02.22 15.06.30.965	System Into System Into System Into System Into System Into System Into System Into				
Emails	2013.02.22 15:05:00:951	System Into				
Ereals from Tasks, Watches waiting for sending Received, processed Ereals Ereals waiting for sending Ereals, All officient within the sended	[3371/5712] 22 2 2013 15:08 Summary Test Test Series System Info	8.29, Compressed. (4298 Bytes / 14178 By a	teri), System Into			
Sent Enails - C-Monitor System Messages Sent Enails - Uries and System takin Result Sent Enails - Responses to CM queries Not Sent Enails - Disabled Not Sent Enails - Failed	Dunning Processes: CPU, CPU Time, Henory 264 21:11:20 62 9 09 0:04:14 105 7	y Usage, Henory Usage Feak, F HD 60 HD 24 HD-80 HD 173 HD 55 HD-60 (1)	end:Write MS, (Dend:Write M Explorer.EXE Semplore.exe	S change), S Normal 31 Normal 51	DG name, Priority, 1 ekonom 1 ekonom 2	Session, User, Bights, Path C:\Bindown C:\Froman Files\Internet Taplorer\
1 History	24 0:22:14 222 1	NB 229 NB 1712 NB-BW (0)	OUTLOOK. BOR (*)	Normal S1	ekanom 3	C:\Program Files\Microsoft (ffice)01
Executed Tanks C-Monitor Execution, C-Monitor Log History Watches History System Into Network Into Waling Tanks History Execution Falls C-BachupPhar Logs C-BachupPhar Logs C-Insige Logi C-verwBackup Logs	14 1:14:134 134 14 14 1:14:21 40 1 14 1:14:21 40 1 14 0:02:39 22 1 04 0:53:50 55 1 04 0:32:43 7 04 0:23:23 13 1 04 0:22:41 11 04 0:12:24 13 04 0:15:24 13	Int         Jo         No         No	Introduct.ess Drug.ecs BofgEng.ess Houtor.ess Searchindeser.ess spolare.ess snapiseditor.ess rochort.ess Acdre.ess FORME-1.EC	Normal 31 Normal 30 Normal 30 Normal 30 Normal 30 Normal 30 Normal 30 Normal 30 Normal 30 Normal 30 Normal 30	donom 2 system 4 system	<ul> <li>C. (Mindows) (System 2011)</li> <li>C. (Mindows) (System 201)</li> <li>C. (</li></ul>
	04 0:14:48 8 1	180 77 285 0 180-547 180 14 299 0 190-547	Access Connections.ese BisTuv.ese	Normal 51 Normal 30	SCOTT REALICE	C:\Program Files\Hierosoft Security +

Obrázok: Prehľad spustených procesov cez uloženú krátkodobú históriu v System Info v C-MonitorConsole

# Spúšťanie programom s admin.oprávneniami u používateľov "user" (funkčné aj na terminálových serveroch)

Mnohí administrátori tvrdia, že je nutné používateľom priradiť administrátorské oprávnenia, ak na počítači je program, ktorý korektne nefunguje bez admin. oprávnení alebo používatelia chcú robiť operácie, ktoré admin. oprávnenia vyžadujú. S C-Monitor-om už toto neplatí, lebo dokáže korektne spustiť program v profile používateľa "user" s oprávneniami administrátora. Je to stav, ktorému by sa ľudovo povedalo : Vlk bude sýty a ovca celá.

Spustenie programu vyžadujúceho admin.práva u používateľa, ktorý má odopreté admin.práva je ilustrovaný na BLOG článku **OpenVPN pre ne-admin používateľa** [6] Date:

3.3.2012External Links:

<u>Spustenie programu vyžadujúceho admin.práva u používateľa, ktorý má odopreté admin.práva</u> [6]Obrázky:



#### Odkazy

[1] https://customermonitor.sk/ako-funguje-cm/monitoring-a-diagnostika/uvod-do-nastavenia-online-monitoringu-watches



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

[2] https://customermonitor.sk/ako-funguje-cm/monitoring-diagnostika/prenesene-data-cez-internet-internet-bandwith-monitor

[3] https://customermonitor.sk/ako-funguje-cm/monitoring-a-diagnostika/volby-a-nastavenie-watchov/prehlad-podmienok-conditions-watc#Internetiptraffic

[4] https://customermonitor.sk/ako-funguje-cm/monitoring-a-diagnostika/volby-a-nastavenie-watchov/prehlad-podmienok-conditions-watc#InternetIPTransferredData

[5] https://customermonitor.sk/ako-funguje-cm/cm-vnutorna-architektura/c-monitor-windows-klient/system-network-info

[6] https://customermonitor.sk/news/blog/openvpn-pre-ne-admin-pouzivatela

[7] https://customermonitor.sk/sites/default/files/OS\_zona\_registracne\_info\_Historia.png

[8] https://customermonitor.sk/sites/default/files/Watches\_condition\_Unauthorized%20Admin%20Pro cess.png

[9] https://customermonitor.sk/sites/default/files/Internet\_bandwith\_Monitor\_prehlad\_prenosov\_po\_ap likaciach.png

[10] https://customermonitor.sk/sites/default/files/System\_info\_spustene\_procesy.png