

Инструкции за инсталиране на софтуерно приложение - SIEM



Инсталиране на софтуерно приложение - SIEM

Инструкции за клиенти

I. Минимални Системи Изисквания:

- 1. NET Framework 4.0+;
- 2. Windows 7 x64+;
- 3. Windows 7 обновен до КВ3033929 и КВ2533623;
- 4. Двуядрен процесор;
- 5. 2GB оперативна памет (RAM).

II. Инструкции за инсталация:

- 1. Отворете линка предоставен в имейла, за да изтеглите приложението.
- 2. Разархивирайте приложението, което изтеглихте от линка.
- 3. С десния бутон на мишката натиснете върху "Sparkguard-SIEM-Agent-

Installer-X.X.exe" и изберете опцията "Изпълни като администратор"





4. Софтуерното приложение ще се зареди на екрана Ви, след което следва да попълните името на групата на Вашата организация, за да може да се свържете към облачния мениждър. Името на групата на Вашата организация можете да намерите в имейла, който получихте в първата стъпка.

Setup - Sparkguard SIEM Agent version 1.2	(777) (777)	
Sparkguard SIEM Agent settings Please specify the settings as per instructions given		CyberLe
SIEM Agent Settings		
SIEM Server Node:		
0f81e7c06665.cloud.wazuh.com		
Server Node Password:		
okVHJjM6o7SHeltYzucvwQGhogB78x9p		
SIEM Group name:		
default		
	Next >	Cancel

5. След като попълните необходимата информация, моля натиснете бутона

Next > _____, за да пристъпите към следващия етап на инсталацията.

6. Потвърдете, че искате да инсталирате пакета **SIEM Agent** и изчакайте 20 секунди, за да завършите инсталирането.

7. За да проверите дали инсталацията е била успешна следва да потвърдите следното:



✓ В прозореца за процесите на компютъра потърсете за ossec-agent.exe



✓ В прозореца за сървиси/услуги за Sysmon

Processes Performance App history Start	up Users	Details	Services				
Name		PID	Descri	iption	Status	Group	^
SNMPTRAP			SNMF	Trap	Stopped		
🔍 Spooler		2392	Print S	Spooler	Running		
Q sppsvc			Softw	are Protection	Stopped		
SSDPSRV		3544	544 SSDP Discovery		Running	LocalServiceA	
SstpSvc		1448	Secur	e Socket Tunneling Protoco	Running	LocalService	
StateRepository		2140	State	Repository Service	Running	appmodel	
🖏 stisvc			Winde	ows Image Acquisition (WIA)	Stopped	imgsvc	
🗟 StorSvc			Storag	ge Service	Stopped	LocalSystemN	
Svsvc			Spot \	/erifier	Stopped	LocalSystemN	
Swprv			Micro	soft Software Shadow Copy	Stopped	swprv	
SynTPEnhService		2796	SynTF	Enh Caller Service	Running		
Sysmon		10136	i Sysmo	on	Running]
🖏 SystemEventsBroker		936	Syster	n Events Broker	Running	DcomLaunch	
🔍 TabletInputService			Touch	Keyboard and Handwritin	Stopped	LocalSystemN	
🖏 TapiSrv			Teleph	nony	Stopped	NetworkService	
鵒 TermService			Remo	te Desktop Services	Stopped	NetworkService	10
🔆 Themes		1808	Them	es	Running	netsvcs	
🔅 TieringEngineService			Storag	je Tiers Management	Stopped		-
🔍 tiledatamodelsvc			Tile D	ata model server	Stopped	appmodel	
Sa TimeBrokerSvc		1328	Time	Broker	Running	LocalServiceN	
🖏 TokenBroker		1808	Web A	Account Manager	Running	netsvcs	
Ski TrkWks		1184	Distrik	outed Link Tracking Client	Running	LocalSystemN	
🖄 TrustedInstaller			Winde	ws Modules Installer	Stonned		Y

8. В случай, че **ossec-agent.exe** или **Sysmon** липсва се обадете на центъра за обслужване на клиенти на Кибер Уан:

✓ 02 4049 840

или изпратете e-mail на:

✓ infosec@lev-ins.com