How to collect all services that are currently running in Windows systems?

1. Choose the organization and corresponding account to collect all the services that are currently running in your Windows.

All Organi	zations						Mon May 1 9:11:32 P	M 🙆 🛔 Priyanka Hiren
S SecPod ^	q	86 Total Devices		9 # Windows	Manag s &	ed Devices 8 Junux	0 # MacOS	69 Others
Domain Controllers	Asset Exposure			ď	Vulnerability Management		Patch Management	
SiteX.SecPod	AE	64	91		VM	1712 Critical	PM	On hosts
SiteY.SecPod SiteZ.SecPod		Applica	ations		17114	7812 High	831	9
SecPod Technolo ^	Windows	Linux	MacOS	Others	Vulnerabilities	7202 Medium	Missing patches	To fix
1 Account Network_Scanner_Demo	242	6211	0	38		388 Low		12608 Vulnerabilities
	Posture Anomal	у		ď	Compliance Management		C Endpoint Management	
SU SecPod US 0 Accounts	952 28		8	CM Compli	iance rules 907 Non-compliant	EM 11	Inactive devices	
	Total Ar	nomalies	High An	omalies	Hosts non-compliant 38/80	Assets non-compliant	SanerNow enabled	Newly added

2. Select the Endpoint Management module



3. Click on **Checks** on the right top corner

Nernow Managing	SiteX.SecPod ${\scriptstyle\checkmark}$		•			Q Mon May 1	1 9:11:57 PM 🙆 🛔 Prij	yanka Hirema
						Check	ks Actions Action S	tatus 1
Total Devices 13	1	ISanerNow enabled	Active Devices	Windows 7		∆ Linux 6	⊯ MacOS O	
Newly Added Devices			Q CSV 7 Days 🗸	Not Scanned Devices			٩	CSV 1 Day
Host Name	Group	.↓† Date		Host Name		Group	1 Date	
sp-nagraj-laptop	Windows-Test	2023-04-26 03:18:57 P	H IST	ms1-home-device		Windows-Test	2023-04-26 04:57:19 PM IST	
				qa-debian-11-x64		grp-1.0	2023-04-19 12:34:28 PM IST	
				sp-mscentos1-x86-64		centos	2023-03-17 09:51:05 PM IST	
				sp-nagraj-laptop		Windows-Test	2023-04-29 03:24:26 PM IST	
				sp-nagraj-laptop.localdomain		ubuntu	2023-04-19 08:12:50 PM IST	
Devices Based on Groups			III csv	Devices Based on OS				
				Device (Count			
	21.1%	e grp-1.0		4				
	3.8%	 centos Windov 	vs-Test	2				
					_			
				0		~ ~ ~		
				Debus	Utrum Cent	NICTON NICTO	upun Micros	
All Devices						Search for host name, group	o, MAC or IP Address Q 🔳 csv	TFilter 1
Host Name	Operating System	Processor	Installed Memory (RAM)	System Type	Group	Primary Mac Address	Primary IP Address	Status
ner.second.com/modules/FM/FM	controLisp?command=on	enDetection formation available	No Information available	No Information available	centos	9E-6E-14-07-D5-92	192.168.2.237	.

4. From the drop-down menu, select Windows and Service Management

san	ernow Managing S	iiteX.SecPod \vee		•		Q Mon May 1 9:18:25	PM 🙆 🛔 Priyanka Hiremath 🗸
•	Network Segments	Endpoin	Protection Software	Sensitive Data Detection	System H	Checks	Actions Action Status #
A						Window	s v Service Management v
₽ G•	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	DHCP	Application Management Network Management Patch Management Computer Information Process Management Device Management System Security
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Signal Quality	Service Management User Management Important wissing Patches
	Installed Patches	Updates Marked Hidden	WSUS-SCCM Status	Active Directory Details	BIOS	Disk	Disk Space less than 100MB
	Operating Systems Information	RAM or CPU Threshold	RAM or CPU Usage	Run Command History	Scheduled Programs	System Up-time More than 7 days	Volumes
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass Storage Devices	Account Lockout Policy
san	ernow Managing S	iteX.SecPod 🗸		•		Q Mon May 1 9:12:04	PM 🙆 🌡 Priyanka Hiremath 🗸
san M	ernow Managing S	iteX.SecPod 🗸			_	Q Mon May 1 9:12:04 Checks A	PM () ▲ Priyanka Hiremath ∨ ctions Action Status #
san ●	ernow Managing S	iteX.SecPod ~ Endpoint	Protection Software	Esensitive Data Detection	System He	Q Mon May 1 9:12:04 Checks A	PM O & Priyanka Hiremath V ctions Action Status A Fools
san ∞ ₽	ernow Managing S	iteX.SecPod ~ Endpoint	Protection Software	Eensitive Data Detection	System He	Q Mon May 1 9:12:04 Checks A alth Windows	PM () & Priyanka Hiremath v ctions Action Status (* Tools V Application Management v
san ∞ □ ▲ €	Applications with Unknown Publisher	iteX.SecPod ~ Endpoint Potentially Unwanted Programs	Protection Software Software Licenses	Eesitive Data Detection	System He	Q Mon May 1 9:12:04	PM () ▲ Priyanka Hiremath ↓ ctions Action Status ◆ Tools Application Management ↓ DNS
san © - - - - - - - - - - - - - - - - - -	Managing S Wetwork Segments Applications with Unknown Publisher DNS Cache	iteX.SecPod V Endpoint Potentially Unwanted Programs	Protection Software Software Licenses Network Interfaces	EESensitive Data Detection	System He ARP Cache Wireless Security	Q Mon May 1 9: 12: 04 atth Windows DHC Common Wireless Signal Quality	PM () ▲ Priyanka Hiremath マ ctions Action Status Tools Application Management DNS Important Missing Patches
San em 	Managing S Image: Constraint of the segments Applications with Unknown Publisher DNS Cache Installed Patches	iteX.SecPod V Endpoint Potentially Unwanted Programs Firewall Policies	Protection Software Software Licenses Network Interfaces WSUS-SCCM Status	Comparison Startup Applications Open Ports Active Directory Details	ARP Cache Wireless Security BIOS	Q Mon May 1 9:12:04 Checks A aith Windows Unix Windows DHC Common Wireless Signal Quality Disk	PM () Artion Status () Action Status () Tools Application Management () DNS Important Missing Patches Disk Space less than 100MB
san ♥ ₽ 8	Installed Patches Operating Systems	iteX.SecPod > Endpoint Potentially Unwanted Programs Firewall Policies Updates Marked Hidden RAM or CPU Threshold	Protection Software Software Licenses Network Interfaces WSUS-SCCM Status RAM or CPU Usage	Emittive Data Detection Startup Applications Open Ports Active Directory Details Run Command History	ARP Cache Wireless Security BIOS Scheduled Programs	Q Mon May 1 9: 12: 04 Checks A alth Windows Unix Unix DHC Common Wireless Signal Quality Disk System Up-time More than 7 days Carlows	M Image: Construction of the second seco

5. Followed by scrolling down, the checks are highlighted in green. Select Running Services

Sanernow Managing SiteX.SecPod ~				•		Q Mon May 1 9:12:13 PM	🚫 🌲 Priyanka Hiremath 🗸
EM						Checks Actio	ns Action Status 🖷
•	Installed Patches	Updates Marked Hidden	WSUS-SCCM Status	Active Directory Details	BIOS	Disk	Disk Space less than 100MB
▲ ₽ C•	Operating Systems Information	RAM or CPU Threshold	RAM or CPU Usage	Run Command History	Scheduled Programs	System Up-time More than 7 days	Volumes
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass Storage Devices	Account Lockout Policy
	Antivirus Information	Data Execution Prevention Status	Faulty Anti-Virus Status	Password Policy	Security Events	Shared Resources	System Events
	User Access Control UAC	Deviation in Co-existing Services	Running Services	Administrator Accounts	Auto-logon Enabled Users	Groups	Guest Accounts
	Inactive Users	Last-logon Users	System Users Identification				

6. To schedule the query execution for the agent, click on **Trigger**. You need to fill up query trigger settings:

• Set the Query run count time in seconds.

sar	nernow	Managing SiteX.SecPod ~				Q Mon May 1 9:12:45	PM 🔘 🛔 Priyanka	
EM			Query Trigger Settings			× Checks /	ctions Action State	is 👘
۲	Name	Running Services - Windows	Query run count	2	<pre>time(s)</pre>	2	V	-
₽.	Description	Collect all services that are cu	Run query every	1	minute(s)		Submit	
		_	Schedule options					
▲	Result Pane		How often	🔿 Immediate 🔿 Daily 🛞 Weekly	/ O Monthly O Date	Search	۹ ۵	lcsv C
₽				Run Every Selected Weeks	weeks on Selected Days - days			
e.		1.0	Query Trigger Time Frame	HH ¥ MM ¥ AM ¥ - HH ¥ MM	I 🗸 AM 🗸		Devic	es
	Devices	0.5		00 00 01 02 03 04 05		Jpdate Close		
				06 Service Name 07 08				
	service_dis	playname IA service_r	name I service_dependency	Ut sen 10 scription	† service_starttype 👫 a	service_status 👫 Hosts	11 Device Names	
	Adobe Acroba	t Update Service AdobeARM	service	Adol 11 12 t Updater keeps your Ado		SERVICE_RUNNING 1	ms-win-test3	
				13				
	Possible Act	ions	ice start type automatic Service start type	15 16 17 18 ▼	Actions			
	Service sta	rt type manual Service start	Service stop					

- Set the time in minutes to run the query often.
- In Schedule options pane, set the **Query Trigger Time Frame**.

• Click on **Update**.



8. Click on the '**Scope**' to choose the scope of the query.

9. To send the query to agent, click on '**Submit**'.

10. In the **Result Pane**, you can view all services that are currently running in Windows systems. You can also download the CSV format of the result pane.



11. You can take possible actions according to the results. Possible actions are specified at the bottom pane. Click on the desired action, you will be redirected to **Create Response page**. In **Created Actions**, you will find all the responses created for the following check.

Create Response Operating System Family* Mindows Ations Ations Create Response Ations Create Response Ations Create Response Create Response	ernow Managing SiteX.SecPod ~	•	🔍 Mon May 1 9 : 13 : 16 PM 🔘 🛔 Priyanka Hiremath 🗸
Create Response Operating System Family* Windows Artise Service reasore			Checks Actions Action Status 💏
Operating System Family* Windows Action* Service remove Service r	Create Response		+
Wadows nume* Actions* Service remove Service re	Operating System Family*	Response Name*	
Action* Service remove Cervice remove Service start type automatic Service start Serv	Windows 🛩	name *	Create Response
Action to restant Service restant Service restant Service stant type submanici AusSvc 256433 AusSvc 256433 AusSvc 256433 AusSvc 256433 Service stant type submanici Service stant type submanici <	Action*	Response Description*	
Service relation Service start type attaining: Service start type attaining: <t< td=""><td>Contract remove</td><td>Action for Running Services - Windows</td><td> Clear Fields</td></t<>	Contract remove	Action for Running Services - Windows	Clear Fields
AarSve_d509c ACPI AcpDev acpicage acpicage acpicage acpicage AcpPmi acpicage ACPIVPC	Service start type automatic Service start type daabled AurSvc_44c86 AurSvc_44c86 AurSvc_5564a33 AurSvc_seA90 AurSvc_bea83	2 Q	 □ Enforce as a rule / Apply always. How often ● Immediate ○ Daily ○ Weekly ○ Monthly ○ Date
acpipag acpipagr AcplPmi acpitume ACPIVPC AcplOne	AarSvc_d50fc ACPI AcpiDev		
accipage AcgriPmi acgritime AcgriPmi A	acpiex		
AcpvPmi acpitime AcpvVPC AcpvVPC	acpipagr		
spitime ACPIVPC ACPIVPC	AcpiPmi		
	acpitime		
	□ ACPIVPC		

Now you know how to collect all services that are currently running in Windows systems.