How to collect DNS information on Windows systems?

To collect all DNS information in Windows systems, follow the steps below:

- Sanernow Managing SiteX.SecPod ~ Q Fri Dec 30 3:24:36 PM 🚫 🔺 Priyanka Hiremath 🗸 Checks ۲ Total Devices C SaperNow enabled Active Devices **Windows** A Linu: ∉ MacOS 8 8 6 4 4 0 Newly Added Devices Q ECSV 7 Days ~ Q ECSV 1 Day ~ Not Scanned Devices A 11 Date 11 Date Host Name Group Host Name Group aifyubuntu-2 ubuntu 2022-12-23 03:58:39 PM IST desktop-cf8v9og windows 10 2022-12-15 01:13:03 PM IST 2022-12-28 05:17:32 PM IST Win10 n-ubuntux64-14 new_group5 2022-12-15 01:36:28 PM IST Devices Based on Groups I CSV Devices Based on OS CSV Device Count ew_group5 3 2019 ubuntu noun MAC or IP Address Q FICSV T Filter 15 -All Devices
- 1. Go to **Endpoint Management** module in SanerNow.

- 2. Click on Checks.
- 3. On the right-hand side, from the drop-down list select 'Network Management'.

sar	nernow Managing	SiteX.SecPo	d v					🞗 🛛 Mon Jan 2 11 : 11 : 28 AM 🛛 🙆 🔺 Priyanka Hiremath 🗸		
•	Network Segments		Endpoint Protection Software		Sensitive Data Detection	System He	Checks System Health		ctions Action Status 4	
▲								Windows 🗸	Network Management 🗸	
e C•	Applications with Potentially Unwanted Unknown Publisher Programs		Software Licenses	Startup Applications	ARP Cache	ARP Cache DHCP		Application Management Network Management Patch Management Computer Information Process Management Device Management		
	DNS Cache	DNS Cache Firewall Policies		Network Interfaces	Open Ports	Wireless Security	Wireless S		System Security Service Management User Management 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 U thar	lp-time More 17 days	Volumes	

sa	nernow Managing	SiteX.SecPod 🗸			Q Mon Jan 2 11	1:11:32 AM	🛞 🛔 Priyanka Hiremath 🗸		
EM				Checks Actions Action Status					
•	Network Segments	Endpoint	Protection Software	Sensitive Data Detection	System He	System Health		Tools	
▲						W	Windows 🗸	Network Management 🗸 🗸 🗸 🗸 🗸	
<i>₽</i> C•	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache		Nindows .inux Mac Common	DNS	
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Signa	al Quality	Important Missing 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-ti than 7 d	ime More lays	Volumes	

4. Select the operating system: **Windows**.

5. The checks corresponding to network management for Windows are highlighted in green.

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

sar	nernow	Managi	ng SiteX.SecPo						O Mon Jar	2 11:12:10 AM	🛔 Priyanka Hire	emath 🗸
EM				Query Trigger Settings					×	cks Actions	Action Status	#
•	Name Description		Nindows omain Name Systen Collect DNS inform	Query run count Run query every		5	* * *	time(s) minute(s)	ž		Submit	+
A	Result Pane			Schedule options How often		Immediate O Daily	O Weekly O	Monthly () Date		Search	Q ICSV	Ċ
₽ G•		2		Query Trigger Time Frame		HH V MM V AM V -	03 ¥ 04 ¥ A	M V			Devices	
	Devices			_					Update Close			
			49.205.72.130	183.82.243.66	8.8.8.8	129.103.4. DNS Serve	169 ar IP	129.103.4.39	129.103.4.167	129.103.4.41		
												•
	Possible Acti	ions inUp					Created Acti					
	Copyright © 2008-2022	SecPod Tech	nologies. All rights rese	rved.							Ve	rsion 5.2.1

• Set the Query run count time in seconds.

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



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

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

9. In the **Result Pane**, you will be displayed with DNS information on Windows systems.

10. 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.

Sanernow Managing SiteX.SecPod ~	•	🔍 Mon Jan 2 11:31:27 AM 🍈 🔺 Priyanka Hiremath 🗸
EM		Checks Actions Action Status 🖷
Create Response Create Response Vindows Sub task*	Response Name* name *	Create Response
Bystem CleanUp ✓	Action for DNS - Windows	Clear Fields
Clan cache v Sub Category* DNS Cache v	C. • centos • ubuntu • Win10 • Windows 10 • windows server 2019	How often Immediate O Daily O Weekly O Monthly O Date
Copyright © 2008-2022 SecPod Technologies. All rights reserved.		Version 5.2.1.5

Now you know how to collect DNS information on Windows system.