How to collect all Dynamic Host Configuration Protocol (DHCP) information on Windows systems?

To collect all Dynamic Host Configuration Protocol information in Windows systems, follow the steps below:

1. Go to **Endpoint Management** module in SanerNow.

	naging SiteX.SecPod		•		Check	3:24:36 PM 🚫 🌲 Priyani	ıs 🐔
₽ Total De 8	vices	© SanerNow enabled	□ Active Devices	₩Windows 4	∆tinux 4	€ MacOS O	
Newly Added Devic	:es		Q CSV 7 Days 🗸	Not Scanned Devices		٩	CSV 1 Day 🗸
Host Name	Group	.↓↑ Date		Host Name	Group	Date	
saifyubuntu-2	ubuntu	2022-12-23 03:58:39 PM IS	т	desktop-cf8v9og	windows 10	2022-12-15 01:13:03 PM IST	
sp-nagraj-laptop	Win10	2022-12-28 05:17:32 PM IS	т	qa-custom-ubuntux64-14	new_group5	2022-12-15 01:36:28 PM IST	
Devices Based on G	Sroups		T CSV	Devices Based on OS			III CS
Derrees babea on e	i o apo			Device Count			
		 centos new_grou 	ıp5	4			
	25%	 windows ubuntu 	server 2019	3			
		 windows Win10 	10	1			
	25%			0 Upunt	Cento Micros.	Micros Micros	

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

Managing SiteX.SecPod V								🛞 🛔 Priyanka Hiremati
	Network Segments Endp		Protection Software	Sensitive Data Detection	retection System Health			s Action Status 🖷
ľ						w	/indows 🗸	Network Management
	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
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Signa	l Quality	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 Up-tin than 7 da		Volumes

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

an	ernow Managing	SiteX.SecPod 🗸				Q Fri Dec 30 3:24:50 PM	🛞 🔺 Priyanka Hiremath 🗸
						Checks Actio	ns Action Status 👫
	Network Segments Endpoint P		Protection Software Sensitive Data Detection		System He	alth	Tools
						Windows ~	Network Management 🗸 🗸 🗸 🗸
	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	Windows Linux Mac Common	DNS
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Signal 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-time More than 7 days	Volumes

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:

• Set the Query run count time in seconds.

sa	nernow Managing	SiteX.SecPod 🗸	A	O Fri Dec 30 3:25:23 PM	🛔 Priyanka Hire	emath 🗸
EM		Query Trigger Settings		× cks Actions	Action Status	ŵ
	Name DHCP - Win Description Collect all I	dows Query run count Dynamic Host (Run query every	5 * time(s) 7 * minute(s)	ź	y Submit	+
	Result Pane	Schedule options How often	Immediate O Daily O Weekly O Monthly O Date	Search	Q IIIcsv	¢ ^
		Query Trigger Time Frame	HH V MM V AM V - 04 V 07 V AM V			
			PM	date Close		ļ
						×
	Possible Actions Network connection kill	Set Static IP Address	Created Actions			
	Copyright © 2008-2022 SecPod Technolog	gies. All rights reserved.			Ve	rsion 5.2.1.5

- 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.

sa	nernow Managing SiteX.SecPo	od ~		Q Fri Dec 30	3:25:37 PM	🛔 Priyanka Hire	math 🗸
EM		Select Groups/Devices		×	cks Actions	Action Status	- 16
0	Name DHCP - Windows Description Collect all Dynamic Host Result Pane	> centos > new_group5 > ubuntu > Win10 > Windows 10		Type here to search ×		Submit	•
 _≎		Windows server 2019		Update Close		C. Inicov	
							•
	Possible Actions Network connection kill Set Static I	IP Address	Created Actions				
	Copyright © 2008-2022 SecPod Technologies. All rights re-					Ve	rsion 5.2.1.5

- 8. To send the query to agent, click on '**Submit**'.
- 9. In the Result Pane, you will be displayed with DHCP information on Windows systems.

Name Descripti		CP - Windows lect all Dynamic Host C	onfiguration Protocol (DHCP) i	information on Windows syst	tems.	т	* rigger	Scope	y Submit	
					_					
4				_					1	
	le Actions work connection	n kill Set Static IF	P Address			Created A	tions			

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.

Nernow Managing SiteX.SecPod ~					Checks Actions	Action Status
					checks Actions	Action Status
Create Response						
Operating System Family* Windows	~	Response Name*				
windows	÷	name *			Create Response	
Action*		Response Description*				
Network connection kill	~	Action for DHCP - Windows			Clear Fields	
					Ciela Picius	
				How often	ily () Weekly () Monthly (○ Date
IP Address*			Q,	Contraction () Du	, O , (Call) (, (Calland) (0.2000
		 centos new_group5 				
Local Port*		ubuntu				
		▶ □ Win10				
Remote IP Address*		 windows 10 windows server 2019 				
Remote in Address						
Remote Port*						

Now you know how to collect all the DHCP information on Windows system.