How to check faulty Anti-Virus (AV) status in Windows systems?

1. Login to SanerNow and choose the **Organization** and corresponding **Account** to check faulty Anti-Virus (AV) status in Windows systems.

sanernow Manag					Q Thu May 25 12:1	~~
Total Devices 9	S SecPod 3 Accounts	^	Active Devices	≝ Windows 4	Checks ∆ Linux 5	Actions Action Status 🕈
Newly Added Devices Host Name No data available	SiteY.SecPod SiteY.SecPod SiteZ.SecPod		Q IIICSV 7 Days ↓	Not Scanned Devices	Group J† Production group	Q III CSV 1 Day > Date III 2023-05-23 11:18:30 PM IST III
G	ST SecPod Techn 1 Account SU SecPod US 0 Accounts	iologies V		qa debian 11.x64 sp-nagraj-laptop. sp-td-win10 sp-ubuntu-ms1	grp-1.0 ubuntu Windows-Test ubuntu	2023-04-19 12:34:28 PM IST 2023-05-09 05:01:50 PM IST 2023-05-10 07:54:05 PM IST 2023-05-24 10:00:40 AM IST
Devices Based on Group			Dec.sv	Devices Based on OS	L. CRAD.	JECON.
All Devices				Sei	arch for host name, group, MA	C or IP Address Q 🗟 CSV 🕇 Filter 15 🗸

2. Select the Endpoint Management module

🖵 Total Devices	SanerNow enab	Your sub	oscribed San	erNow tools		& Linux	di Mac	os
9	9	0 7				5	0	
Newly Added Devices		AE	VM	РМ			C	CSV 1 Day
Host Name	Jh Group				II. Group		Date	
No data available					Productio	an group	2023-05-23 11:18:30 PM IST	
					grp-1.0		2023-04-19 12:34:28 PM IST	
		PA	CM	EM	ubuntu		2023-05-09 05:01:50 PM IST	
				sp-td-win10	Windows	-Test	2023-05-10 07:54:05 PM IST	
				sp-ubuntu-ms1	ubuntu		2023-05-24 10:00:40 AM IST	
Devices Based on Groups			CSV	Devices Based on OS				6
44.4%	22.2%	ubuntu grp-10 Windows-Test Production group		3 2 1	utor Marine			

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

sar EM	Nernow Managing	SiteX.SecPod ~		•	Q	Thu May 25 12:14 Checks	: 58 PM	
•	Network Segments	Endpoint	2 Protection Software	Sensitive Data Detection	System He		Actions	Action Status #
∎						Wind	lows ~	Application Management 🛛 🗸
<i>₽</i> G•	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	DHCP		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 M days	ore than 7	Volumes
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass Storage	e Devices	Account Lockout Policy

4. From the drop-down menu, select **Windows** and **System Security**

sa	nernow Managing	SiteX.SecPod \vee			Q	Thu May 25 12:	15:12 PM {	👌 🛔 Priyanka Hiremath 🗸
EM						Checks	Actions	Action Status 🛛 🔗
•	Network Segments	Endpoint I	Protection Software	Sensitive Data Detection	System He	alth		Tools
∃							ndows 🗸	Application Management 🗸 🗸
<i>∎</i> G•	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	Lir Ma	ndows nux ac mmon	DNS
	DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Sign	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		Run Command History	Scheduled Programs	System Up-time days		Volumes
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass Store	ge Devices	Account Lockout Policy

anernow Managin	g SiteX.SecPod ~			۹	Thu May 25 12:	15:15 PM {	🔅 🛔 Priyanka Hiremath 🦄		
•					Checks	Actions	Action Status 🛛 👫		
Network Segment	ts Endpoint	Protection Software	Sensitive Data Detection	System He	alth		Tools		
					w	/indows ~	Application Management 🗸 🗸		
Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	DHCP		DHCP Patch Managemen Computer Informatio Process Management		Computer Information Process Management
DNS Cache	Firewall Policies	Network Interfaces	Open Ports	Wireless Security	Wireless Signal Quality		Device Management System Security Service Management User Management		
Installed Patches	Updates Marked Hidden	WSUS-SCCM Status	Active Directory Details	BIOS	Dis	k	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 Stor	age Devices	Account Lockout Policy		

5. Followed by scrolling down, the checks are highlighted in green. Select Faulty Anti-virus status

an	ernow Managing	; SiteX.SecPod ~			Q	Thu May 25 1:02:19 PM	Priyanka Hiremath
						Checks Actions	Action Status 🛛 🌴
l	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 100MI
	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.

Query run count	5	time(s)	
Run query every	*	minute(s)	
Schedule options			
How often	Immediate O Daily O Weekly O Mo	onthly 🔿 Date	
Query Trigger Time Frame	HH 🗸 MM 🖌 AM 🖌 - HH 🖌 MM 🖌 AM	~	

• Set the time in minutes to run the query often.

ging SiteX,Se	Query Trigger Settings	(C Thu May 25 12:16:34 PM X Actions
int Lockout Pc caccount lock	Query run count Run query every Schedule options	5	<pre>time(s)</pre>	ź
	How often Query Trigger Time Frame		○ Weekly ○ Monthly ○ Date	rch
				Update Close

• In Schedule options pane, set the **Query Trigger Time Frame**.

	Query Trigger Settings			× Actions
Account Lockout Po Theck account lock	Query run count	5	<pre>time(s) </pre>	2
neck account lock	Run query every	7	<pre>^ minute(s)</pre>	
	Schedule options			
	How often		Weekly O Monthly O Date Weeks • Weeks on Selected Days • days	
	Query Trigger Time Frame	HH ¥ MM ¥ AM ¥ -	HH ~ MM ~ AM ~	
				Update Close

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

Managing SiteX.			O Thu May	25 12:17:20 PM
	Select Groups/Devices			× Actions
Antivirus Informatic Checks for Anti-Viru running.	 ▷ grp-1.0 ▷ Production group ▷ ubuntu ▷ Windows-Test ▷ sp-td-win10 ♡ sp-win-2019-server 		Type here to search	×
			Update	Close
		100%		

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

10. In the **Result Pane**, you can check the antivirus_name, path_to_signed_product_exe, product_enabled. product_uptodate, hosts, device_names. You can fetch the results and download the CSV format of the result pane.

11. You can take possible actions like service start, start process, application management according to the results. Click on the possible action, you will be redirected to **Create Response page**. In **Created Actions**, you will find all the responses created for the following check.

sane M	rnow Managing Si	teX.SecPod 🗸					Q	Mon May 1 9 : 32 : 38 PM Checks Actio	
•	Application and Device Control	JuneUp	Software Deployment	D Process	Registry	Service	Network	System	File
e C•	Startup Programs	Security							

Now you know how to check faulty Anti-Virus (AV) status in Windows systems.