## How to list last-logon details of users on Windows systems?

1. Choose the organization and corresponding account to list all guest accounts in Windows systems.

						Manas	ged Devices		
s	5 Accounts		86		9 Windows		8 A Linux	0 MacOS	69 Others
	Domain Controllers		- Total Devices		C			-	others
	Presales- Test Account	Asset Exposure			6	Vulnerability Management		Patch Management	
	SiteX.SecPod	AE	64	91		VM	1712 Critical	P 14	On hosts
	SiteY.SecPod SiteZ.SecPod		Applica			17114	7812 High	831	9
	SecPod Technolo ^	Windows	Linux	MacOS	Others	Vulnerabilities	7202 Medium	Missing patches	To fix
ST	1 Account	242	6211	0	38		388		12608 Vulnerabilities
	Network_Scanner_Demo	_					Low		
	SecPod US	Posture Anoma	y		C	Compliance Management		C Endpoint Management	
SU	0 Accounts	PA				CM	liance rules	EM	Inactive devices
						503	3 907		
		952		2	8	503 907 Compliant Non-compliant		11	6
		Total A	nomalies	High An	omalies	Hosts non-compliant	Assets non-compliant	SanerNow enabled	Newly added
						38/80	13/13		1

2. Select the Endpoint Management module

	80 Total Devices		7		Your sub	oscribed SanerN	low tools	0 MacOS		67
Asset Exposure	Total Devices		I Window	vs	07			MacOS		Others
	36 Applic			5 c 2 a	AE	VM	PM	Windows Cristian Linux	Currently Monitored Applica	tions
Windows 181	Linux 3489	MacOS O	Others 23	29	PA	СМ	EM	Others	2,000 Application Count	4.000
Posture Anomaly				100					Anomalies Confidence Distr	
	<b>52</b> nomalies	Anor	<b>8</b> nalies nfidence)	741 A	nomalies foun nomalies foun malies found ir			5000002 500		20 High
Vulnerability Mar	agement	13	58							
13	591		ical 05		devices have v devices have v		at have known attacks.	10 7	Vulnerability Statistice	Critical High Medium

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

						Check	s Actions Action S	tatus
₽Total Devices 13		D SanerNow enabled	□ Active Devices	Windows 7		∆Linux 6	t MacOS ■	
Newly Added Devices			Q CSV 7 Days V	Not Scanned Devices			٩	CSV 1Da
Host Name	La Group	.↓† Date		Host Name		Jà Group II	Date	
sp-nagraj-laptop	Windows-Test	2023-04-26 03:18:57 PM I	ST	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	,		II CSV	Devices Based on OS				[
5	23.1%	ubuntu     grp-1.0     centos     Windows-	Test	4 Device C				
All Devices					Utturk Cer	Search for host name, group,	MAC or IP Address Q ECSW	<b>T</b> Filter 1
Host Name	Operating System	Processor	Installed Memory (RAM)	System Type	Group	Primary Mac Address	Primary IP Address	Status

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

sai	nernow Managing S	iiteX.SecPod		•		<b>Q</b> Mon May 1 9:12:04 P	M 🔘 🛔 Priyanka Hiremath 🗸
EM						Checks Ac	tions Action Status 希
● 	Network Segments	Endpoint	Protection Software	Sensitive Data Detection	System He	alth	Tools
A						Windows	✓ Application Management ✓
₽ C+	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	DHC 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
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass Storage Devices	Account Lockout Policy

	Inernow Managing Si	iteX.SecPod 🗸				Q Mon May 1		÷	
•	Q		<u></u>		♡	Chec	ks Action	ns Action Status	ñ
	Network Segments	Endpoint	Protection Software	Sensitive Data Detection	System He	alth		Tools	
▲							Windows ~	Service Management Application Management	~
e G	Applications with Unknown Publisher	Potentially Unwanted Programs	Software Licenses	Startup Applications	ARP Cache	DHCF	,	Application Management Network Management Patch Management Computer Information Process Management Device Management System Security	
	DNS Cache	DNS Cache Firewall Policies		Open Ports	Wireless Security	Wireless Signal Quality		Service Management User Management Important Massing 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		Volumes	
	Windows System Metric	Current Processes	Bit-locker Status	Keyboard and Pointing Devices	Storage Devices Connected	USB Mass S Device		Account Lockout Policy	у

5. Followed by scrolling down, the checks are highlighted in green. Select **Last-logon Users**.

sar m	<b>Ternow</b> Managing Si	iteX.SecPod 🗸				Q Mon May 1 9 : 26 : 37 PM Checks Action	
•	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.

sa	nernow	Managing SiteX.SecPod ~	0		<b>A</b>			n May 1 9:12:45 PM	👌 🛔 Priyanka Hi	remath N
EM			Query Trigger Settings				×	Checks Actions	Action Status	- #
۲	Name	Running Services - Windows	Query run count	2	* *	time(s)	1		<i>Y</i>	-
P	Description	Collect all services that are cu	Run query every	1	*	minute(s)			Submit	
			Schedule options							
A	Result Pane		How often	O Immediate	○ Daily	Monthly 🔿 Date		Search	Q. ECS	C
8				Run Every	Selected Weeks • weeks	on Selected Days •	days			
G		1.0	Query Trigger Time Frame	HH ¥ MM ¥	AM 🗸 - HH 🖌 MM 🗸 AM				Devices	
	vices	0.5		00 01						
	De	0.0		02 03 04			Update Close			
				05 06 07 08	iervice Name					
	service_disp	olayname Ih service_n	ame	11 sen 10	cription 💵 se	ervice_starttype	1 service_status	lt Hosts lt D	evice Names	đ
	Adobe Acrobat	Update Service AdobeARMs	enice	Adot 11	t Updater keeps your Ado SE	ERVICE_AUTO_START	SERVICE_RUNNING	1 m	s-win-test3	
				13						
	Possible Act			15	Created Actio					
	Service rem	ove Service restart Servi	ce start type automatic Service start type	17						
	Service star	t 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.

saner	rnow Managing SiteX.Sec	od 🗸	<b>A</b> 0	Mon May 1 9:31:05 PM	💄 Priyanka Hiremat
EM		Select Groups/Devices		× Checks Actions	Action Status 4
Nan	lame Administrator Accoun	v v gop-1.0	Type here to search		<i>7</i>
🖵 Des	Description List all Administrator	count:			Submit
E					Q Elcsv C
A	esult Pane		Update C	Search	Q LEGY C
₽					

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

10. In the **Result Pane**, you can view list all administrator accounts on Windows systems. You can also download the CSV format of the result pane.

inter, name         1         Intel, lagar         1         Intel, lamas         1         Reads         1	of source on Windows systems, Frigger Response Submit	A. Inge	9 11000	Modow getern.	Last logan them. Windows List has logan details of asses on W	tana Neuriptian
Mill 1012 [2019] Administrator No. 1, 2011, 1012 AM 2014 (0.0121) 1 als 4072 (0.012	1. bet, bages 1. bet, bestag, dies 1. beste Barres 1.	1 Andre 1 Andre Annes	1 last, bestag, time	het, begen		
Michigher Strategie Strate	No. 1, 201, 101, 101 M 201 O 40 10, 217 1 also 4070 girls	1 44-07104-0	2012-02-08-02.02.27	Har 11, 2011, 1101 (0.488		
		1 40-07532-00				
MR 1072[070].col 0.011.07 1 al-0723.cl	201-0-00.0.07 1 al-070.046	1 40-0703040	2011-01-08-01-01-07		C C QUE V C LANK	ana 111111
MR 1/17/2019/04/10/phonet 2014/04/11/1 als 4/17/phil	2010-0-00-0.12 I an-077-parts	1 win-01711gball0	2012-01-08-01-01-27		Coperative statistics	ana 111111

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.

	ernow Managing Si	teX.SecPod 🗸			•		٥	Mon May 1 9:32:38 PM	👌 🛔 Priyanka Hiremath 💊
EM								Checks Actions	Action Status 🛛 👫
₽	Application and Device Control	TuneUp	Software Deployment	Process	Registry	Service	Network	System	File
▲ ₽ C•	Startup Programs	Security							

Now you know how to list last-logon details of users on Windows systems.