How to set alerts in SanerNow?

To set alerts, choose the organization with respective account. You can set alerts for individual modules: vulnerability management, patch management, asset exposure, compliance management, endpoint point management, and device management.

Note: Configure your <u>mail settings</u> before you enable the alerts.

- Q Wed Nov 29 6:03:52 PM Sanernow Managing SiteX.SecPod Visibility • Device Universe Cyber Hygiene Score 9 چ **0** 18 🧐 **0** 😰 22 Newly Added Devices Active Devices Inactive Devices Device Groups Operating System 78 23 ▦ 3505 8 74 🏨 **1** 🏨 5 🖧 1 High Total Applications **Outdated Applications** Blacklisted Application Network Subnets User Groups Q Detection Category Risks Severity Trend Affected Devices Launch 34/78 🔞 VМ 6689 •) 813 35/78 СМ 757 •) 64 11/01 23/78 PA 3104 0 РМ •1 316 E Prioritization 👋 RP Prioritized Risks Factors Influencing Risk Prioritization
- 1. Once you choose organization account, click on 'Alerts' on left panel.

2. Choose the module you have subscribed to.

Asset Exposure:

Alerts	~		•		Q Feldan Succ Exposu	essfully subscribed to Asset e alerts
Asset Exposure	Posture Anomaly	Vulnerability Manag Subscription status Send to E-mail* Conditions*	ement Compliance Management ov admin@secpod.com Software License Violation Outlated Applications New Assets	Patch Management Patch Management Rarely-used Assets New Devices Blacklisted Assets	Endpoint Management	Device Management
					Update	

3. Select the **Conditions**. Conditions refers to when an alert must pop up to the given email. Conditions include:

- Software License Violation
- Rarely-used Assets
- Outdated Applications
- New Devices
- New Assets
- Blacklisted Assets
- 4. Click on **Update**.

Continuous Posture Anomaly Management:

Alarts	CitAms09-11-42-04AU 600 Successfully subscribed to threat alerts						
Asset Exposure	Posture Anomaly	Vulnerability Man	agement	Compliance Management	Patch Management	Endpoint Management	Device Management
		Subscription status Send to E-mail*	ON Info@secpor	d.com			
		Detection*	Posture A All Anom Custom D	nomaly Detection ^{alles} etection Rules ²⁵	Custom Detection Custom Detection Rules		
		Response*	 All action All failure 	is e actions	All successful actions Custom Response	lpdate	
						_	

2. Assign the 'Send to E-mail.'

3. Enable All Anomalies detection, if you want to get notified each time whenever a new anomaly is detected. Or you can assign custom detects by entering PA-IDs.

4. Under Custom Detection Rules, you can get notified by all queries of custom detects or you can enter name of the detection rule with comma separation.

5. You get notified if the response of the detects are, All actions, All successful actions, All failure actions, and Custom Response. In Custom Response, add comma separated custom values to get custom alerts.

6. Click on **Update**.

Vulnerability Management:

Sanernow Managing Suraj ~			•		Q Est Anno Succe vulnerab	Setter 2012 AM
Asset Exposure	Posture Anomaly Vulner Subscription status Send to E-mail* Conditions*	OK admin@secpod.com Z All vulnerabilities	Compliance Management	Patch Management	Endpoint Management	Device Management
		 High Fidelity Attack Vuli 	unness Nerabilities Updat	Custom Conditions	NE BANISHED	

3. Select the **Conditions**. Conditions refers to when an alert must pop up to the given email. Conditions include:

- All vulnerabilities
- Critical vulnerabilities
- High and Critical vulnerabilities
- Medium, High and Critical vulnerabilities
- High Fidelity Attack Vulnerabilities
- Custom Conditions: Add comma separated custom CVEs.
- 4. Click on **Update**.

Compliance Management:

Alerts	·		•		C Est Anno Succ complia	essfully subscribed to nce alerts
Asset Exposure	Posture Anomaly	Vulnerability Mana	gement Compliance Management	Patch Management	Endpoint Management	Device Management
		Subscription status Send to E-mail* Conditions*	admin@sscpod.com All compliance checks	Custom Conditions	Update	
					_	

3. Select the **Conditions**. Conditions refers to when an alert must pop up to the given email. Conditions include:

- All compliance checks
- Custom Condition: Add comma separated custom CCEs to get notification.
- 4. Click on **Update**.

Patch Management:

Alerts	✔ Managing Suraj ∨			•		Succe Manager	essfully subscribed to Patch nent alerts
	Asset Exposure	Posture Anomaly	Vulnerability Mani Subscription status Send to E-mail* Conditions*	agement Compliance Management Com admin@secpod.com Detection All Missing Patches Important and Critical Patches Response All actions All failure actions	Patch Management Critical Missing Patches Custom Detection All successful actions Custom Response	Endpoint Management	Device Management

3. Enable detection checkbox, get notified when there is detection of Missing Patches, Critical Missing Patches, Important and Critical Patches, and Custom Detection.

4. Under Response, you can get notified by all queries of custom detects or you can enter name of the detection rule with comma separation.

5. You get notified if the response of the detects are, All actions, All successful actions, All failure actions, and Custom Response. In Custom Response, add comma separated custom values to get custom alerts.

6. Click on **Update**.

Endpoint Management:

Alerts	🕅 Managing Suraj 🗸						C Stillers Succe alerts	sofully subscribed to query
	Asset Exposure	Posture Anomaly	Vulnerability Mana Subscription status Send to E-mail* Conditions*	agement	Compliance Management	Patch Management Custom Query Detection	Endpoint Management	Device Management
				Response All action All failure	ts actions	All successful actions Custom Response	Update	

3. Enable Query detection checkbox, get notified when there is trigger of 'All queries' or you can enter comma separated values for Custom Query Detection.

4. In Response, get notified if the response of the detects are, All actions, All successful actions, All failure actions, and Custom Response. In Custom Response, add comma separated custom values to get custom alerts.

5. Click on Update.

Device Management:

anerno	W Managing Suraj	v			•		Q e Ma	Successfully subscribed to Device nagement alerts
Aierta	Asset Exposure	Posture Anomaly	Vulnerability Man	agement	Compliance Management	Patch Management	Endpoint Management	Device Management
			Subscription status Send to E-mail* Conditions*	admin@se	icpod.com III Agent Lidded Devlces	Scan Finish Inactive Devices	Update	

3. Select the **Conditions**. Conditions refers to when an alert must pop up to the given email. Conditions include:

- Uninstall Agent
- Scan Finish
- Newly Added Devices
- Inactive Devices

4. Click on **Update**.

Now you know how to set Alerts in SanerNow.