USING REDSEAL TO RESPOND TO SUNBURST

RedSeal recently released a high-level overview of how to leverage our product to assist in your investigation, containment, and remediation efforts following the recent activity impacting SolarWinds Orion. As noted in the overview, the following playbook is generally being followed by our customers:

- **Step 1**: Do I have SolarWinds Orion?
- **Step 2**: Where is it, in context of my network?
- **Step 3**: What is it capable of accessing/controlling?
- **Step 4**: Fix Orion or take it offline (if subject to the CISA Emergency Directive).
- **Step 5**: Block unwanted access to or from SolarWinds Orion, to the extent possible.
- **Step 6:** For all assets SolarWinds could reach, reset them to known good state.

RedSeal is helpful in dealing with steps 2, 3, and 5. Using RedSeal, with your other tools, provides relevant information at the various stages of your response efforts.

NOTE: With exception of the Incident Response portion, everything below is accomplished using the RedSeal java client.

Step 1 - Do I have SolarWinds Orion?

To identify SolarWinds Orion hosts in your network model, you can leverage vulnerability scan data or endpoint data. While we are not a software inventory tool by design, the host data contained in our model can help determine types of software and the versions present in the environment based on data such as ports, protocols, and applications.

You may have other tools or manual lists to identify SolarWinds hosts, but we recommend using RedSeal to automate the validation of any other sources.

The latest scans from your vulnerability scanners may not contain information about your SolarWinds devices if they were powered down.

We recommend using the latest CVE scanners with tactics that assume the CVEs are not alerting correctly, also known as trust but verify.

Reports. Within the RedSeal Client, navigate to the Reports Tab. The pane on the left contains the available report designs. For this use-case, you can use the Vulnerability Management report or the Security Model Inventory Report. Within the report template, you can alter the Fields and Filters to include data points such as ports, application name, IP address, hostname, etc.

Endpoint Data. If your endpoint solution supports a .csv export, you can search through this data, after importing, from the Endpoint Data Tab within the RedSeal Client. You can use your endpoint solution export in conjunction with your Vulnerability scan data to search for ports, protocol, applications, or other data points of interest.

API. RedSeal's API can be used by leveraging user-created scripts that enable the retrieval of data from your RedSeal instance and formatted in a manner applicable to your enterprise. For further assistance, reach out to your RedSeal Account Team or reference the User Guide or API Programmer's Guide for details on Reporting, Endpoint Data, or API scripting.

Step 2 - Where is it, in context of my network?

Once SolarWinds hosts have been identified, you can run a series of queries to help understand the location of the system(s), potential impact, and network access of the host(s) on the network.

1. **Incident Response Tab**.
   If you have a known IP address of the SolarWinds Orion host, you can use the Incident Response Tab to locate which switch port the device is plugged into and shut it down. To locate the switch port providing connectivity to the host , log into RedSeal via the web interface and navigate to the Incident Response Tab.
   Note: A Layer 2 License and Layer 2 Data is Required.
   a. Enter the IP address or hostname of the host with SolarWinds Orion and perform a search.
   b. The "Threat Source Overview" pane contains information such as IP address, MAC address, switch port, topology group membership, and other host details. Depending on your network model, you will be able to validate reachability of your SolarWinds host to other topology groups.

2. **Maps and Views Search - Known Host(s)**.
   If you have a known IP address, hostname, or uniquely identifiable string in the hostname for your SolarWinds systems, using the RedSeal Client, navigate to the *Maps & Views* Tab:
   a. On the *Search* sub-tab, enter the IP address or hostname of interest.
   b. From the Results pane, click on the host to show more information or right click and select *Show in Tree*.
   c. From there, you can right click the host and *Pin Host(s)* if you wish to make the hosts viewable on the map.

   You are also able to add the hosts to their own Topology Group which can be used as a source or destination for additional queries, Zones & Policy analysis, or reports.

Step 3 - What is it capable of accessing/controlling?

Access Queries and Zones & Policy Analysis are foundational capabilities within RedSeal. We recommend having Zones and Policies defined, consistent with your organization's security policy. During an active incident, SolarWinds hosts, for example, could be placed in their own topology group and/or zone to simplify analysis and provide better answers to management.

1. **Access Queries**
    a. Inbound query: In the *Maps & Views* Tab, in the left pane, select *Subnets* on the View drop-down and select *Untrusted*, right–click, *Explor*e, *Access From* - this will identify all inbound access from all untrusted network space.
    b. Outbound query: Following CISA's directive to block external access from SolarWinds, you can use RedSeal's Access Queries to validate that SolarWinds hosts cannot communicate externally. In the *Maps & Views* Tab, select the SolarWinds hosts Topology Group, right–click, *Explore*, *Access From* - this will identify all outbound access from the SolarWinds hosts - the Blast Radius.
    c. Access or Threat Queries run from the *Security Intelligence Center* can search on Layer 7 App IDs. This adds another method of screening for SolarWinds Orion access potential. ***Note: Supported Layer 7 firewalls include Check Point and Palo Alto.***

2. **Zones & Policy**
    a. Within the client, navigate to the *Zones & Policy* Tab, *Manage Policy Sets*, name the policy, ensure the box to *Activate Policy* is checked, click *Save*.
    b. Right click in the blank center panel and select *New Zone* or click on the *New Zone* Hyperlink, name the Zone SolarWinds, click *Save*.
    c. Repeat step *b.* but name the Zone Untrusted.
    d. Click on the SolarWinds Zone, click the *Add* button in the bottom pane. *Search* or *Browse* to find your previously identified SolarWinds hosts and click the *Add to Zone* button
    e. Click on the Untrusted Zone, click *Add*, and click the *Browse* Tab, change the view from *Topology* to *Subnets* in the drop-down menu, and select the *Untrusted* folder and *Add to Zone*
    f. Click the directional dashed line from SolarWinds to Untrusted and click the *Edit Rules* button. Check the box for *Enable Access Rule* and the radio button for *All Access Forbidden* and *Save*. Repeat for the directional dashed line from Untrusted to SolarWinds. Click the button for *Update Compliance*.
    g. Green arrows indicate there is no access from the defined source and destination zones. Red arrows indicate that access is allowed between source and destination zones and should be investigated.

Step 4 – *Fix Orion, or take it offline*

As referenced in step 1, you can use the *Incident Response* Tab to locate the switch port you want to shut down or disconnect. If the SolarWinds host is believed to have been shut down, disconnected, or quarantined, you can use the Layer 2 modeling to validate that SolarWinds hosts are, in fact, unreachable.

Step 5 - *Block unwanted access to or from SolarWinds Orion*

** Use analysis from step 3 to determine which devices need to be reconfigured to block access.**

1. If you've pinned the SolarWinds host, right-click on the pinned host in the Topology map or if you have not pinned the host, navigate to the host in the left pane of the *Maps & Views* Tab and choose *Explore*, *Set as Source*
2. Click on *Explorer* text in the icon bar to bring up the Explorer window
3. Click on *Advanced Query*
4. In the *Security Intelligence Center* window click the *Select* button under *Destination.* Click on the *Browse* Tab and choose *All Untrusted Subnets* and then click the *Replace* button
5. Click the *Detailed Path* button at the bottom of the window. This will open the *Detailed Path* window. Any device in the lower left *Selected Detail Path* section that is highlighted is allowing access. Clicking on the device will populate the *Filter/NAT Rules and Routes For Device* panel in the lower right corner of the window. The line in the configuration for that device will be listed and can be given to the device admin to shut down the access. For more detail, you can right click the rule and *Show in Config File.*

Step 6 – *For all assets SolarWinds could reach, reset them to known good state*

Follow the guidance of your organization to wipe and rebuild your assets.