December 20, 2021

Dear Customer,

The purpose of this message is to outline the steps you can take using your RedSeal system to:

1. Get the list of hosts and devices that have the Log4j vulnerability
    a. This list can be exported into a ticketing system or provided as a spreadsheet to your mitigation teams
2. Gain visibility into the access from and to Untrusted Sources to the vulnerable hosts and devices
3. Use the actionable insights to put in place compensating controls to mitigate the risk

RedSeal is aware of the recent vulnerabilities related to Log4j, and RedSeal Classic software is not vulnerable. You can find more details about this on the RedSeal website https://www.redseal.net/redseal-response-to-log4j2-vulnerability/ and also contact our RedSeal support at support@redseal.net if you have more questions.

This note applies to customers using RedSeal and importing vulnerability data into RedSeal from scanners and the customer.

Prerequisites:

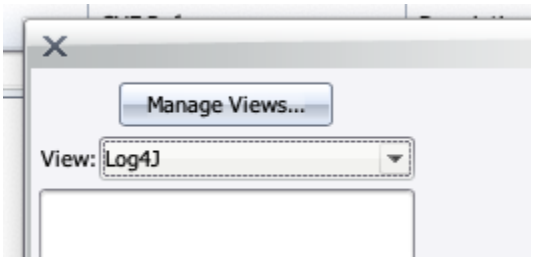
1. Updated the scan vendor's product so that the Scan Library includes the Log4j Vulnerabilities CVE-2021-44228, CVE-2021-45046, and CVE-2021-4104
2. Completed either a partial scan, or ideally a "Full Scan" of the network
3. Downloaded the latest RedSeal TRL that includes the above-mentioned vulnerabilities
    a. This was published on the RedSeal Support site on 12-17-2021 at 2pm Pacific Standard Time
4. Perform a Data Collection task on your Scanner
5. Run RedSeal analysis

The following steps show the processes to identify vulnerable hosts and devices, and then show Untrusted Source access to hosts and devices, and also the access from the hosts and devices to an untrusted destination. This is important in being able to prioritize your mitigation efforts.

The Methodology is called Discover Investigate and Act. In the case of Log4j: **Discover** infected devices and host, **Investigate** access paths to and from untrusted areas, and then provide data to immediately **Act** upon.

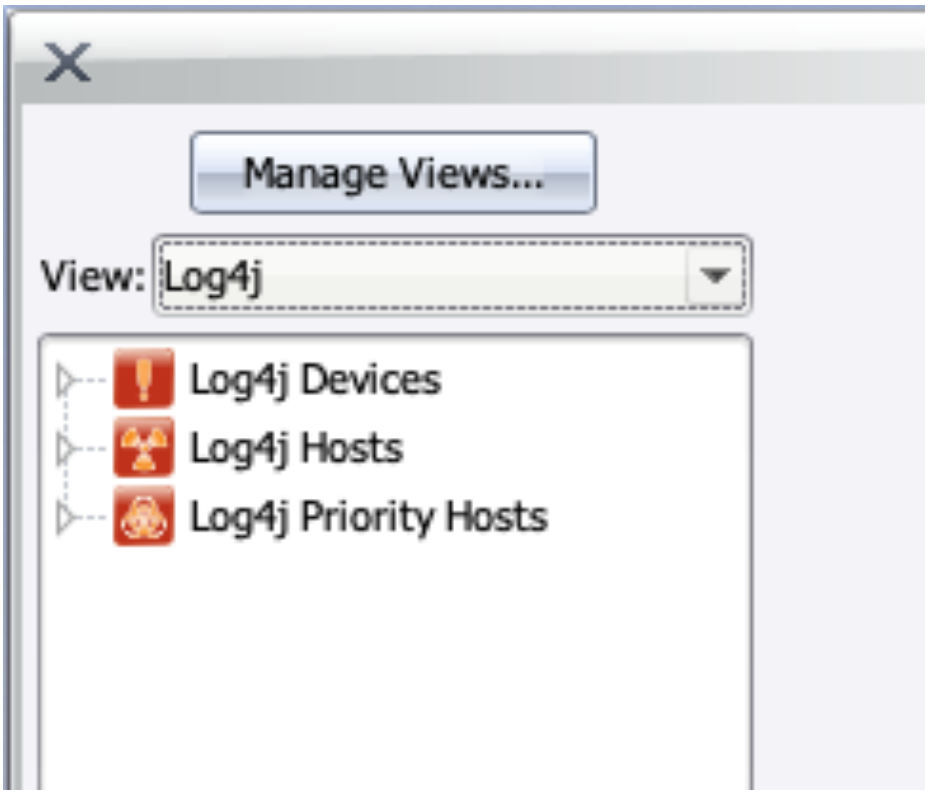
Step 1:

In RedSeal Client, navigate to → Tools, Manage Views and Groups.
Create a View and call it Log4j.



Step 2:

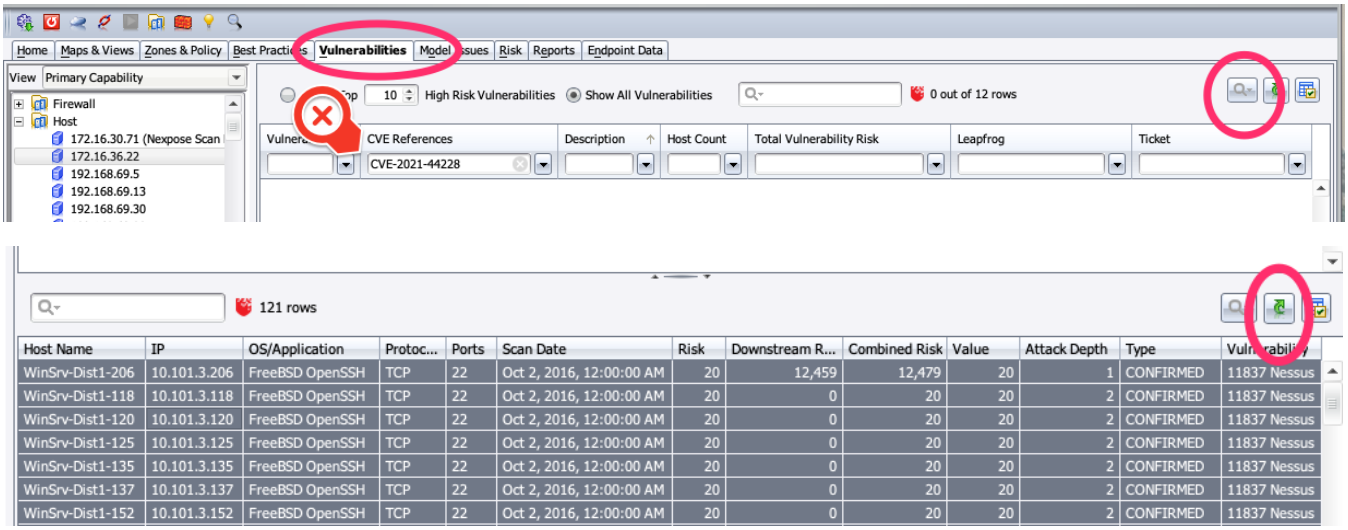
In the view, create two groups call Log4j Devices, Log4j Hosts, and Log4j Priority Hosts. Tricks and Traps: after you make the first group, you need to click on the View name again, or the second group will appear as a sub-group to the first group.

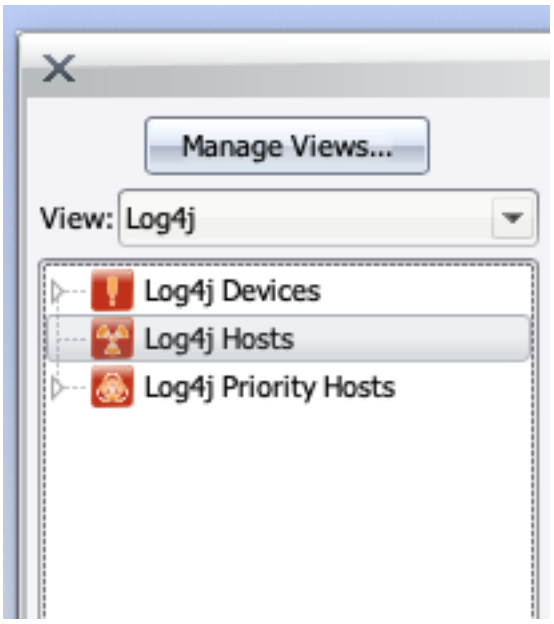


Step 3:

Identify all hosts that your vuln scanner identified by searching for the three CVE's: CVE-2021-44228, CVE-2021-45046, and CVE-2021-4104. Click the Vulnerabilities Tab, click the show all Vulnerabilities radio button, then click the magnifying glass on the far right to allow a column search. In the CVE Reference column enter the first Log4j CVE – first screenshot (ss). In the bottom Details pane, you will see a list of Hosts that have the Vulnerability. There are two things to do here:

1. Sort the list in descending order by business value to prioritize which to patch first. Click the green export arrow on the far right to export the list of hosts to a file in the Tab Separated Values (TSV) format that can be read by excel. Provide this list to your mitigation/patching teams
2. Right click on any host in the Details pane, click select all, right click again and select Host details. In the corresponding list, click any host, right click, select all, right click and "Copy to Group." Browse through the Views until you find your Log4j View, then select the Log4j Host group, then click the Add selection to group button – second ss.

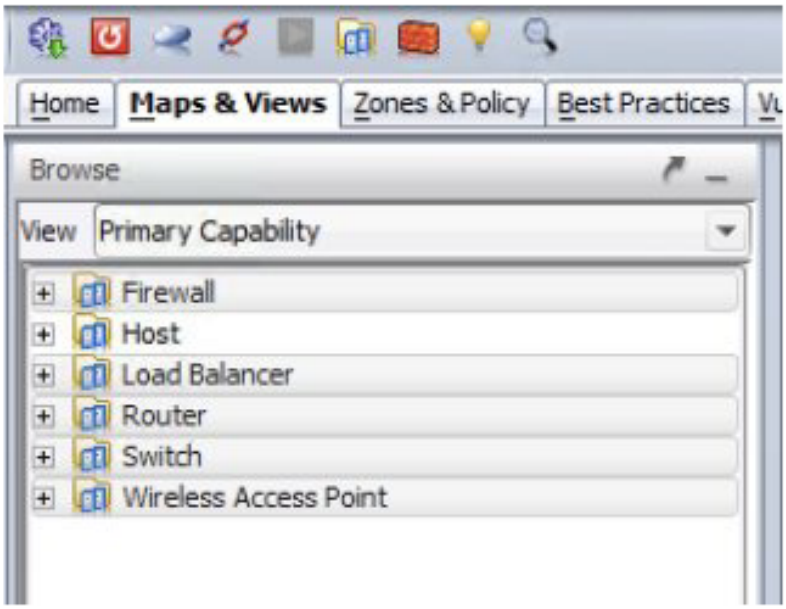




Step 4:

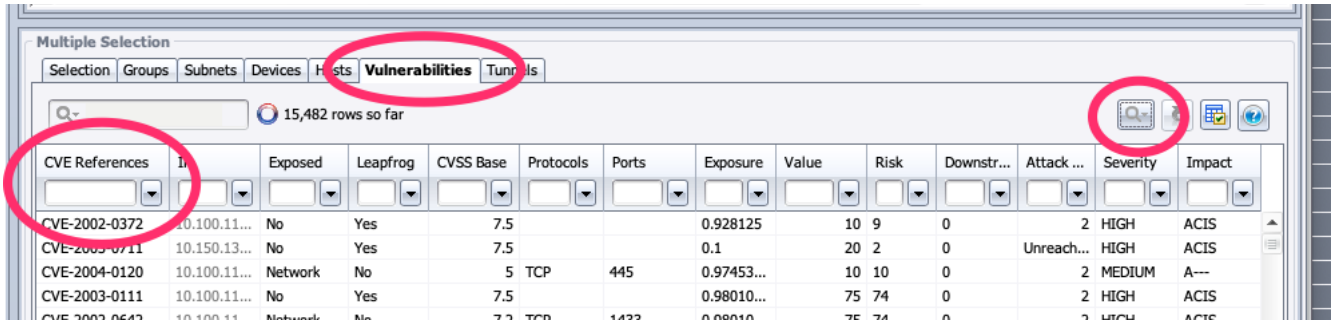
Now for the Devices.

Go to Maps & Views tab, select View of Primary Capability, select everything BUT Hosts:

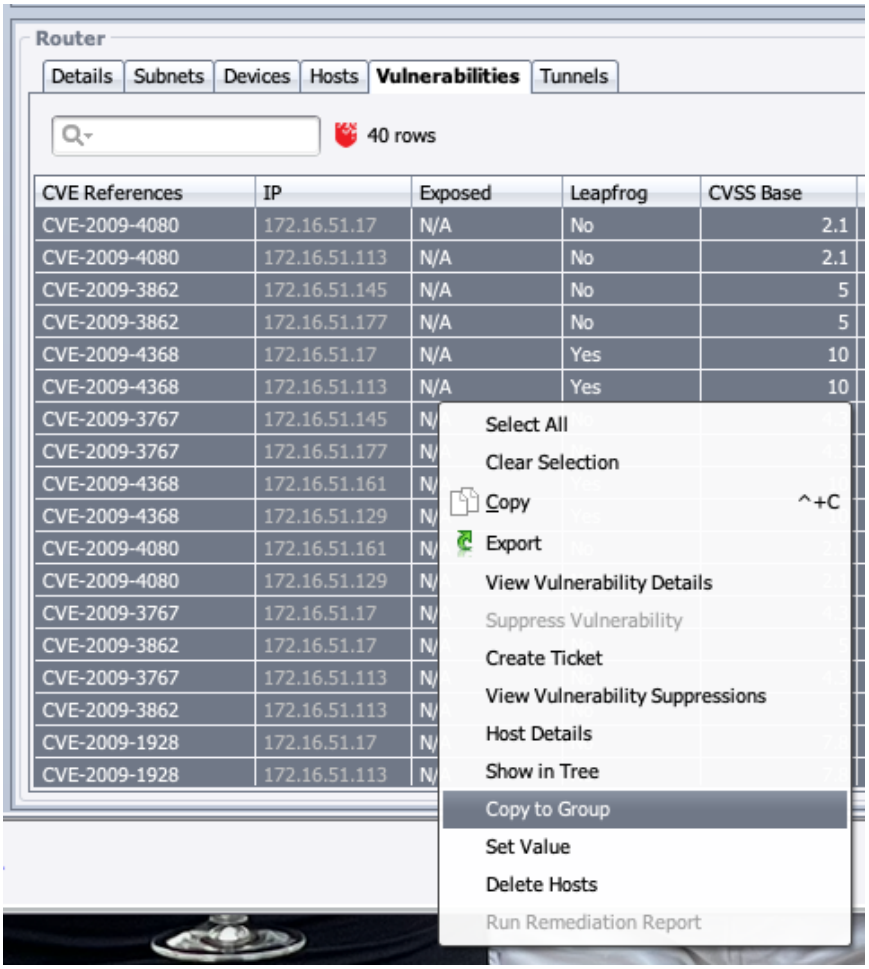


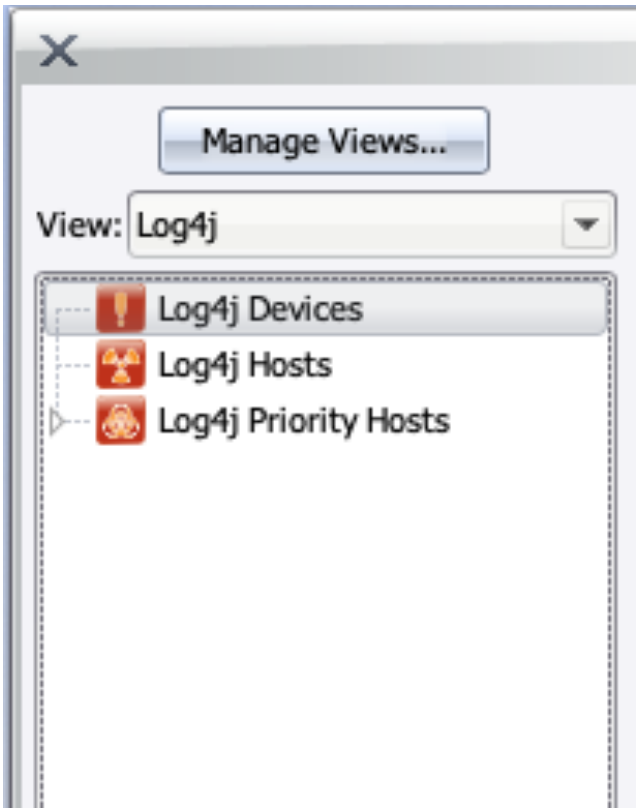
In the Details Pane under the Map select the Vulnerabilities tab:

As it's populating (which can take a WHILE) select the magnifying glass on the right icon to open up the search field for each column and put in the reference for the first CVE. Yes, you're going to have to do these one CVE at a time. You may have to hit ENTER in this field again, after the selection is done to refresh the search.



After the list is populated, select one of the results, then right click and choose Select All. Then right click and select Copy to Group. Navigate to the Log4j view, and select the Log4j Devices Group – second ss.

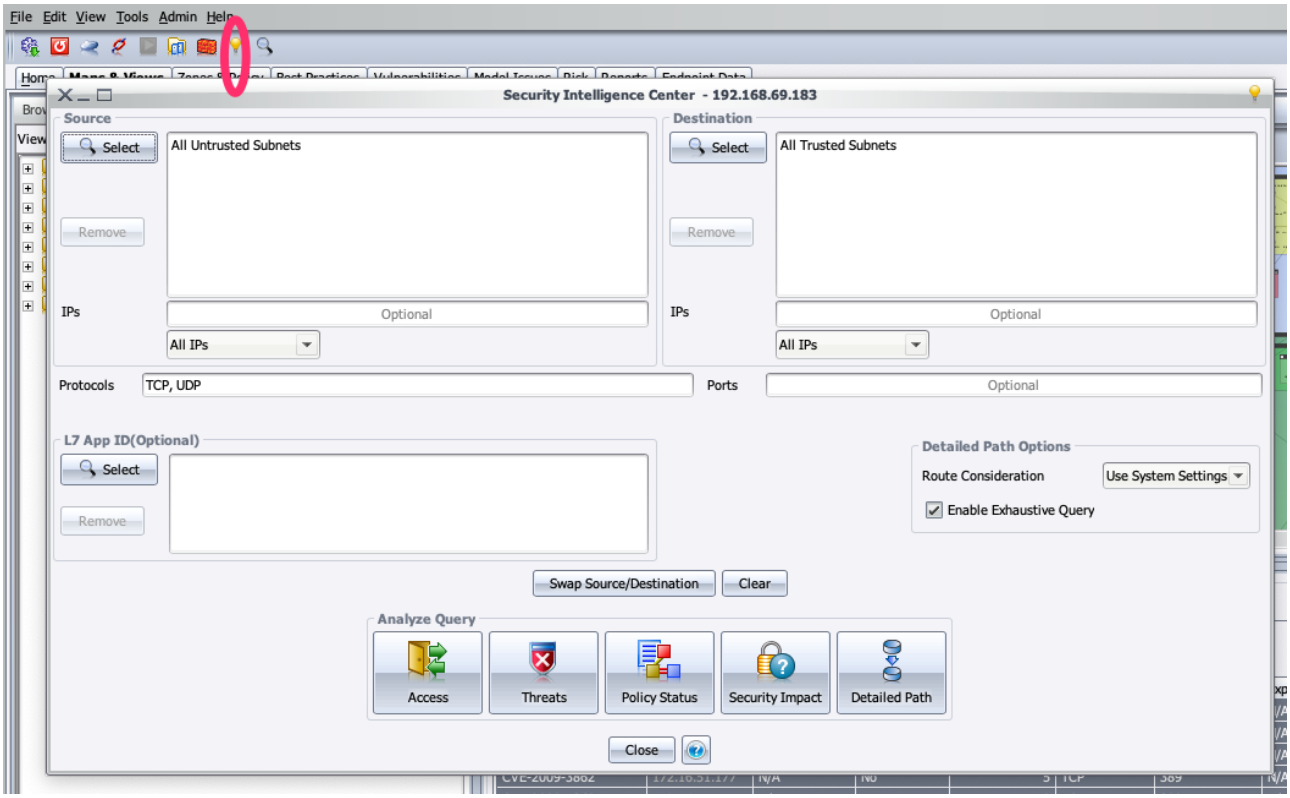




Step 5:

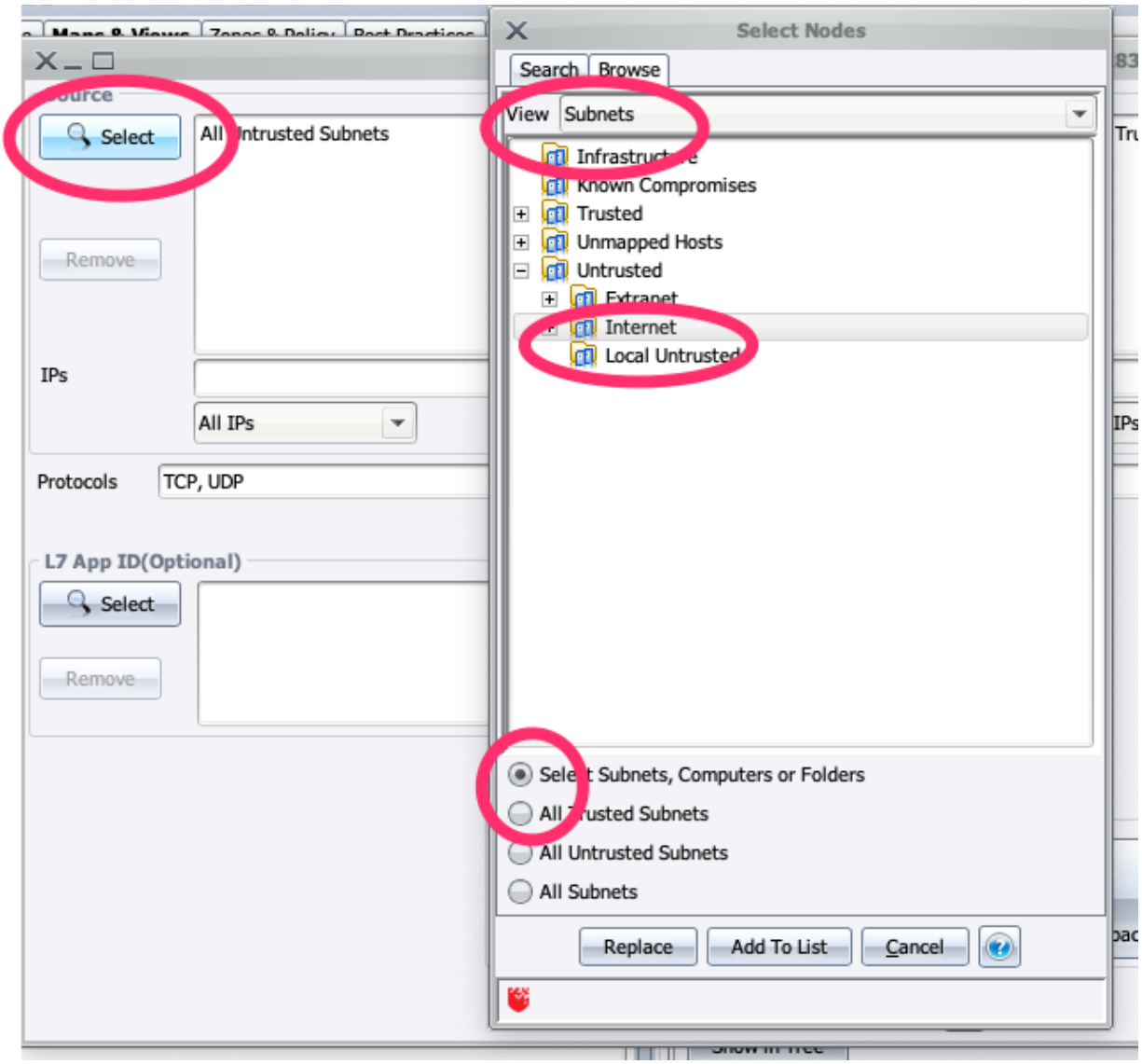
Access queries

Click the light bulb on the top icon bar to get the Security Intelligence Center

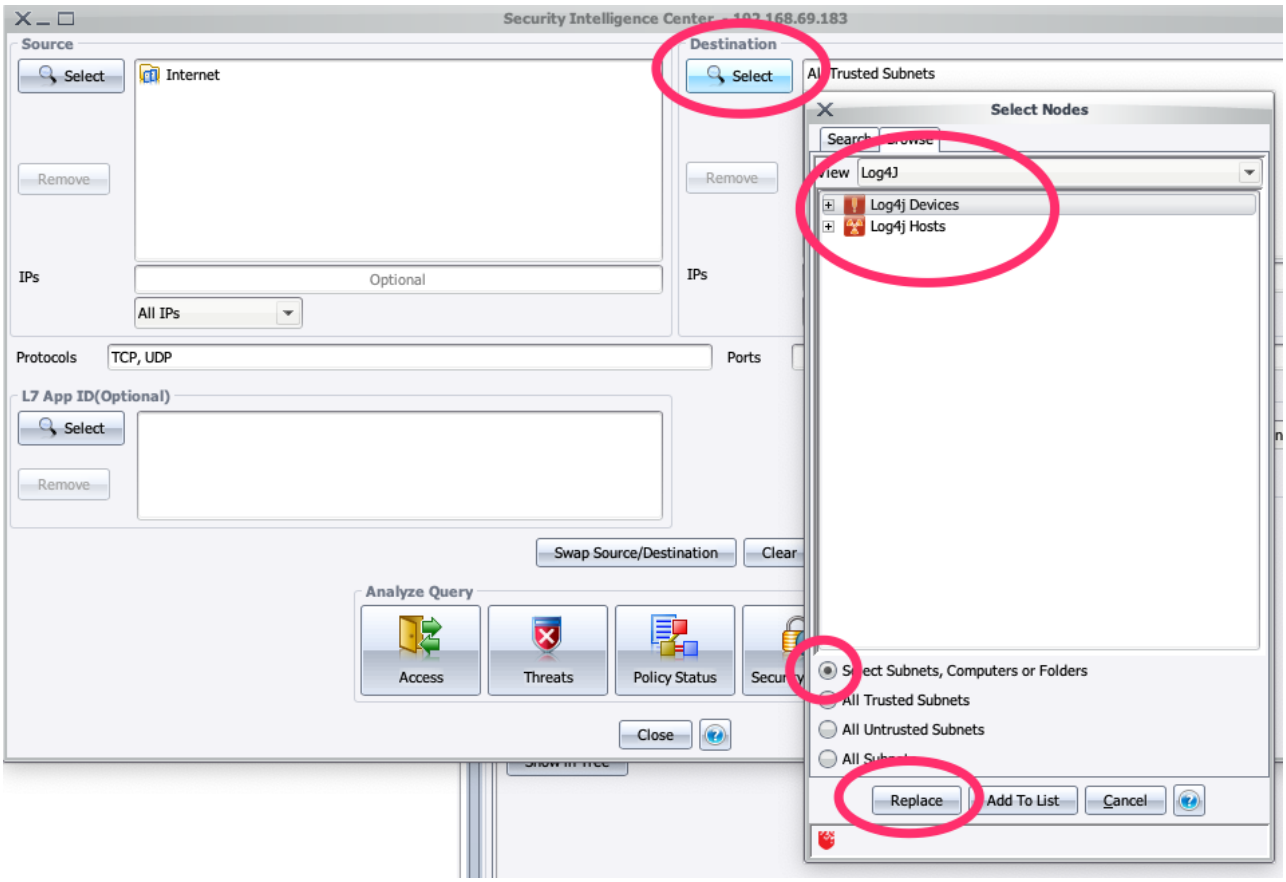


Now we need to select the Source and Destination of either the Device or Hosts Log4j Group. For each destination we will run four Access Queries. One from the Internet, one from the other Untrusted Sources: Local Untrusted and Extranet, and lastly, the third query is the Reverse. Because the Log4j vulnerability is a two-step process, the infected host or device must initiate a second connect outbound to deliver the payload. Thus, it cannot take advantage of a stateful, inbound connection. This is a way to prioritize which devices/hosts to patch first. In this case, the ones that have access TO an untrusted destination.

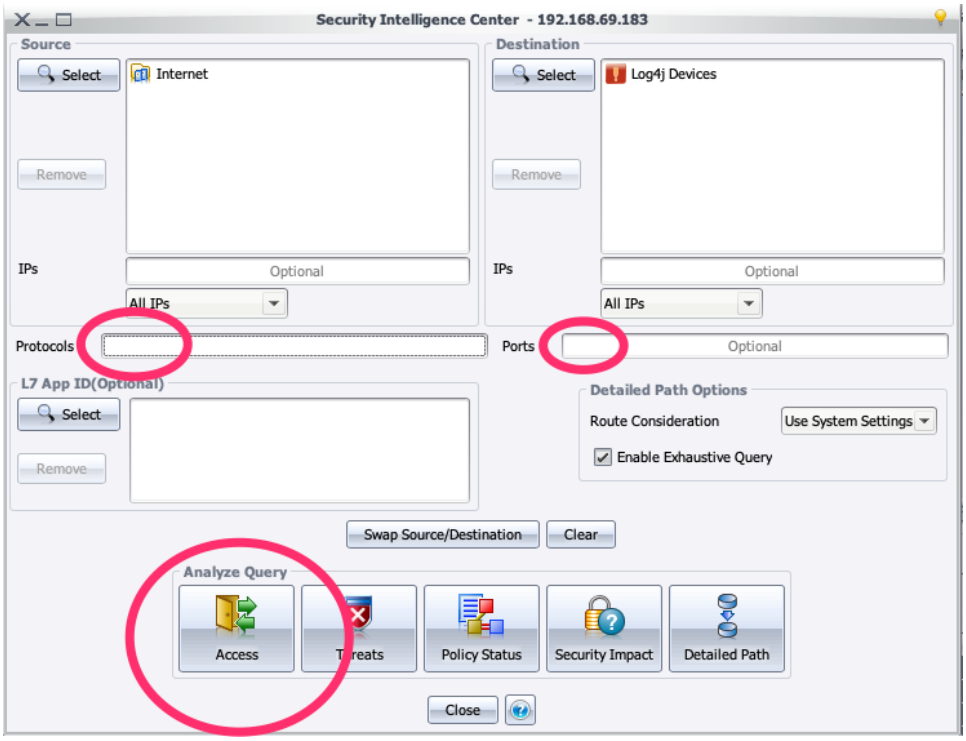
Click the select button in the upper right, on the bottom of the resulting dialogue box click the radio button that says “Select Subnets, Computers or Folders, then change the View on the top to subnets and Select Internet, then click the Replace button on the bottom.


Select
All Untrusted Subnets
Remove
IPs
All IPs
Protocols
TCP, UDP
L7 App ID(Optional)
Select
Remove
Select Nodes
Search
Browse
View
Subnets
Infrastructure
Known Compromises
Trusted
Unmapped Hosts
Untrusted
Extranet
Internet
Local Untrusted
Select Subnets, Computers or Folders
All Trusted Subnets
All Untrusted Subnets
All Subnets
Replace
Add To List
Cancel

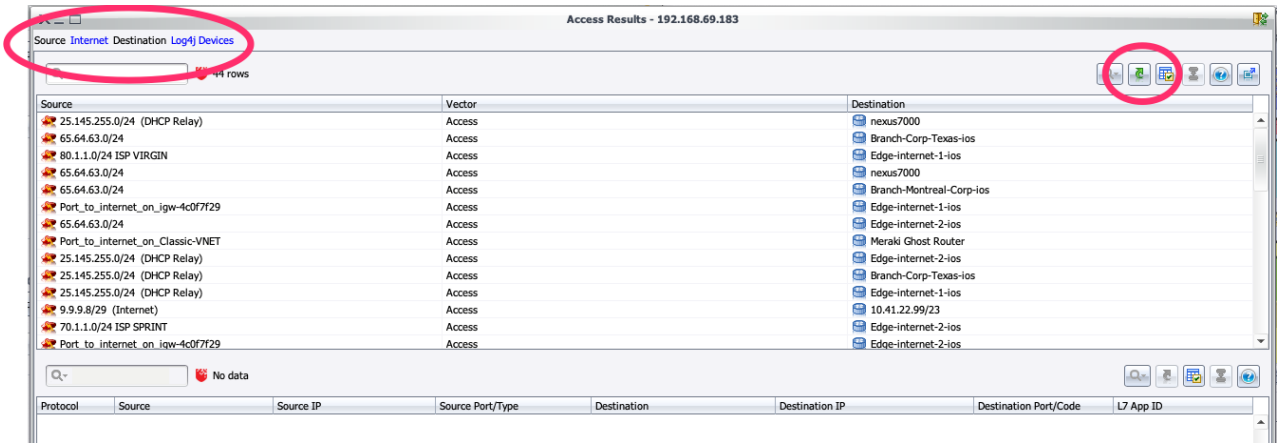
Now click the Select button on the Destination (right) side of the dialogue box, click the Select Subnets, Computers and Folders radio button, change the view to the Log4j Devices and click the Replace button.



Now, clear the Protocols and Ports fields. You could argue that only TCP, and a limited set of ports would be needed, but any access “may/cold” get logged. Click the Access button.

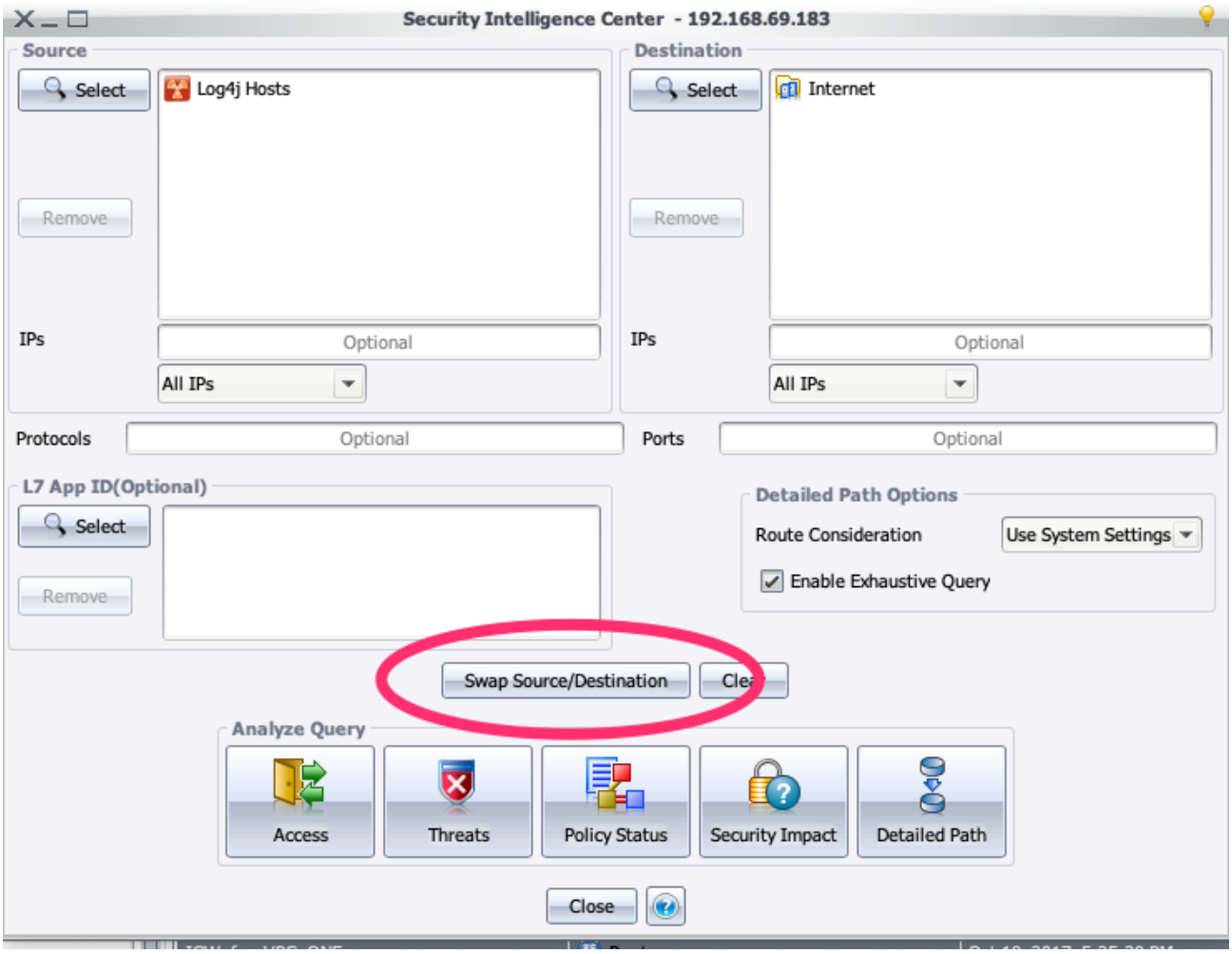


The result is a list off all Devices that have the Log4j Vulnerabilities that are accessible from the Internet. An audit of this list for critical devices is warranted. The list can be exported by click the green arrow on the right. Perform the same process with the other Untrusted sources: Local Untrusted and Extranet. Also perform the same queries, but change the destination to the Log4j Hosts group.



Once you have performed these queries and exported the results, you can prioritize the Host list by reversing the query.

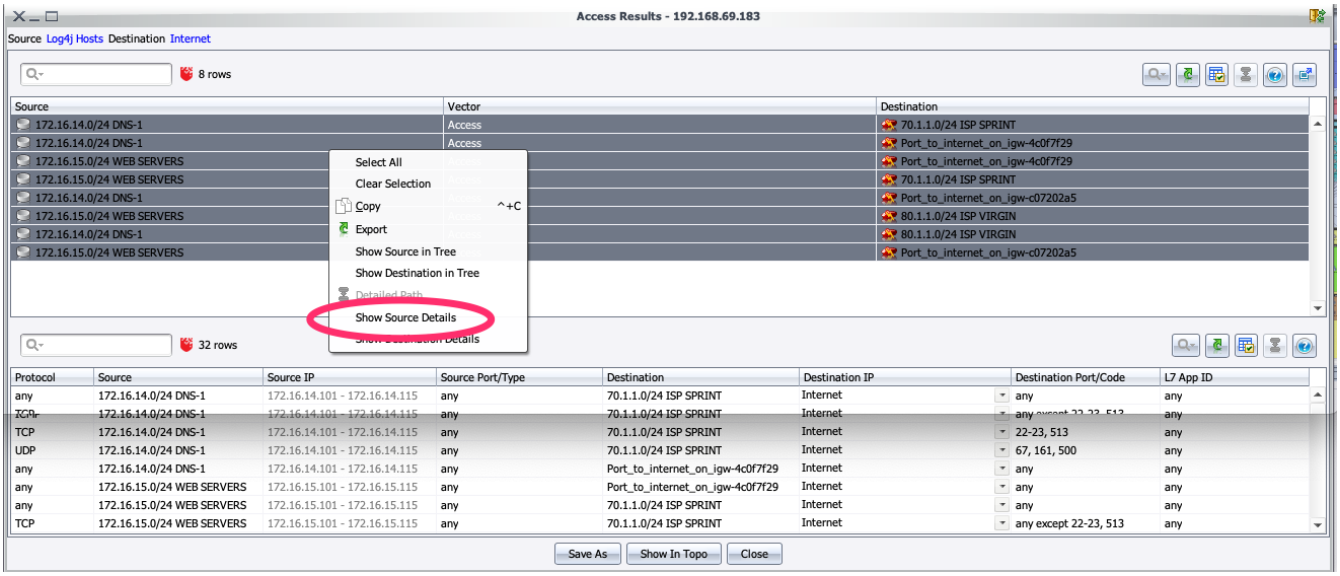
Go back to your original Security Intelligence Query screen and select the Swap Source/Destination and click the Access Button.



The resulting list is much smaller, and are the ones that are not only vulnerable, but exploitable. This is a powerful finding because we know that a stateful connection to a host cannot be used to deliver the outbound payload of from the host. Therefore, this is the list of hosts to patch first, or setup logical or physical network segmentation from the Untrusted source. Once these are mitigated, then move onto the remainder of the list.

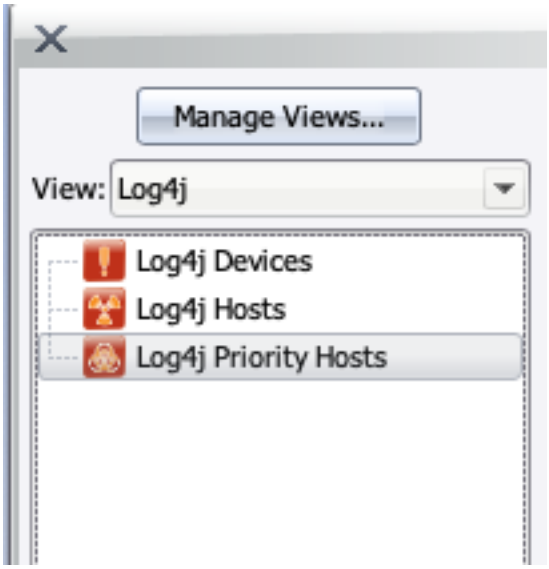
In order to get the Actionable data to perform the logical or physical network segmentation, we need to take this smaller list and add it to the Log4j Priority Hosts group we made early on.

From the results table of the query from the Log4j Hosts to the Internet/Untrusted, click in the top pane, right click and select all, then right click and select Show Source Details.



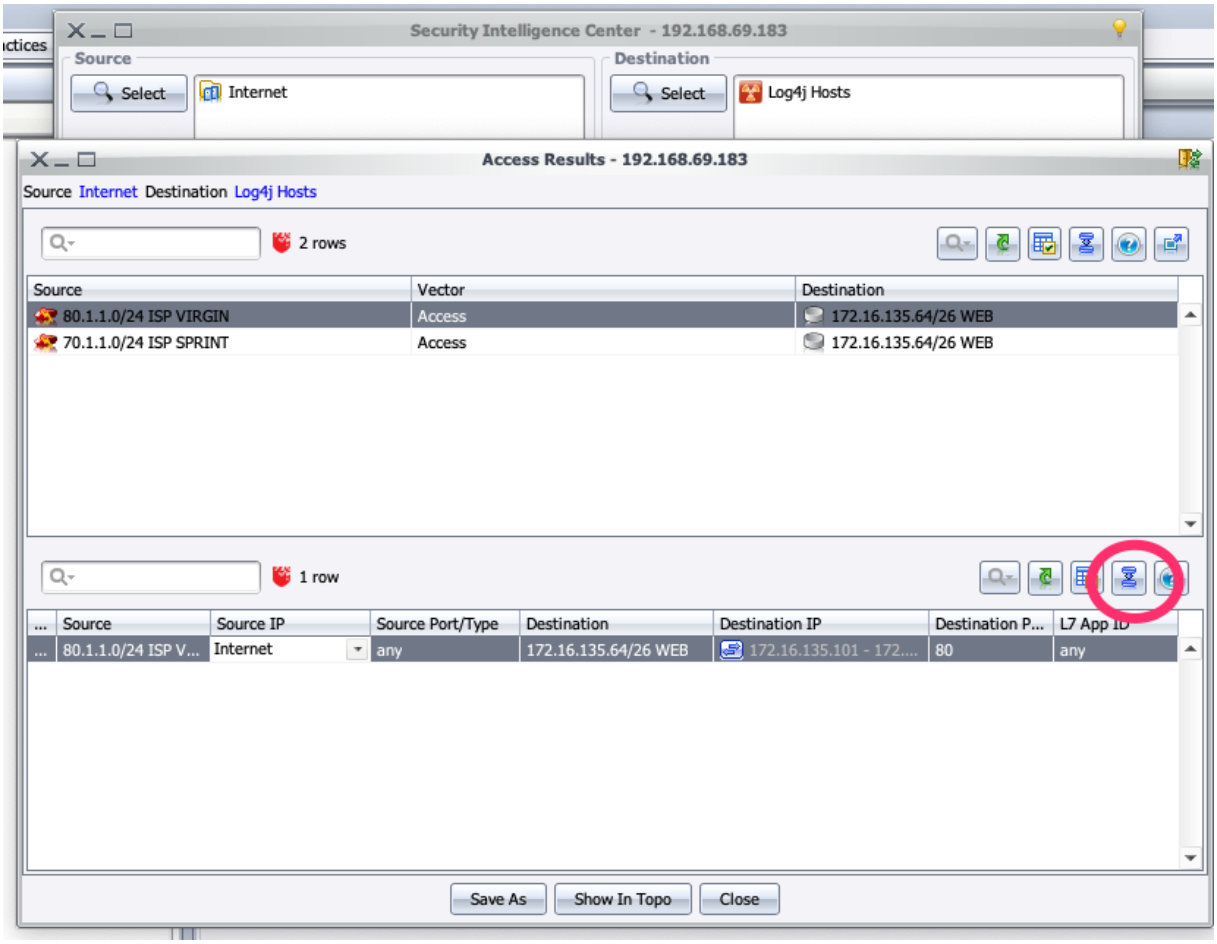
Then click the Hosts tab, click in the table below, right click, select all, right click, select Copy to Group, select the Log4j Priority Hosts group, and Add.

You now have lists of Devices, Hosts, and Prioritized Hosts that can be given to your Mitigation Teams.

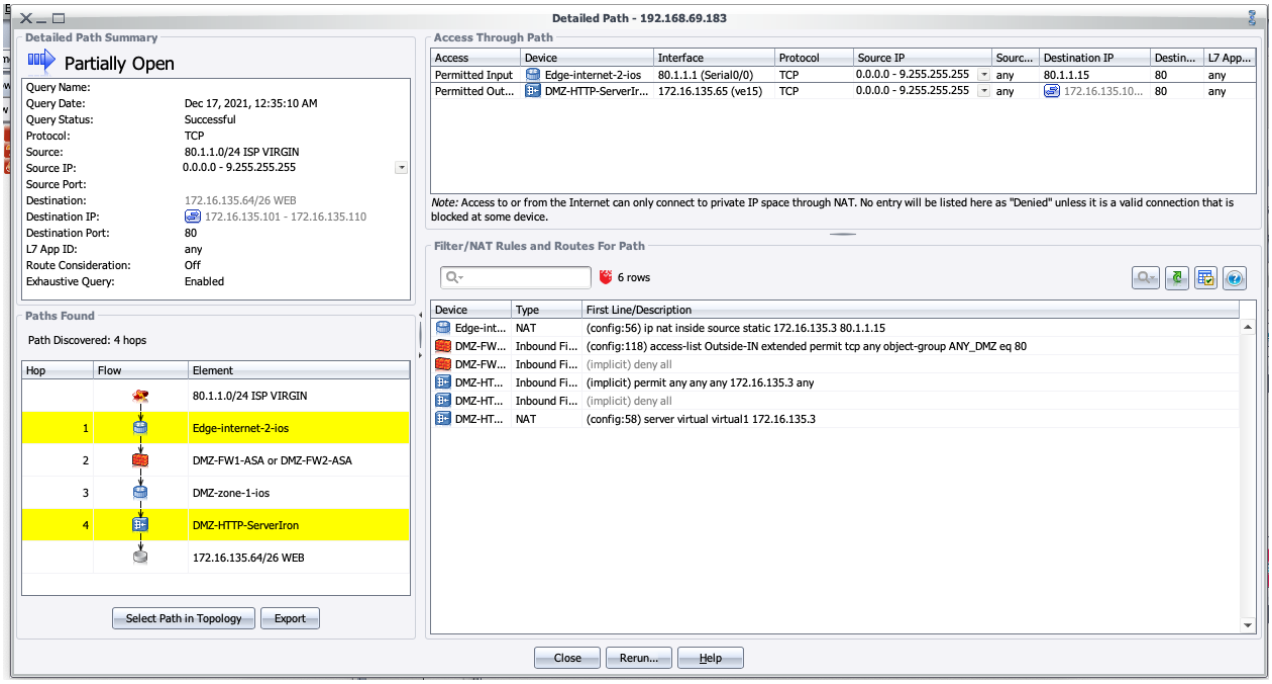


Next is to get the actionable Access Data for your Network teams to create logical or physical barriers from Untrusted sources like the Internet.

From any of the query results table, select an Access Result in the top pane, then click a row in the bottom pane and either click the Detailed Path icon, or right click and select Detailed Path.



The resulting Detail Path shows a Subway map on the lower left of all the Hops from the source to the destination, on the right are the details of the entire path, and all the Access Control (ACL's) Lists in the bottom right pane. If you click and hop on the subway path, it will show you the specific ACL that is allowing, limiting, or blocking the traffic. This information is what is needed by your Network teams. The top priority would be to provide these results for the Outbound query from the Prioritized Host list.



In Summary:

The Actionable data for a host is the Host name or IP. However, the Actionable data for the access comes from a Detailed Path Queries as explained in the last portion of this document.

By following the above steps, you have created three sets of Actionable Data:

1. A list of all infected hosts that can be given to the patching team
    a. Hint, break them out by Topo Group so the different teams in different regions get a scrubbed list
2. A list of all access to infected devices to be given to the network team so they can perform logical, and if needed, physical segmentation on the network to remove the access
3. Hop by Hop details of all paths into and out of your network that could be used by the Log4j Vulnerabilities