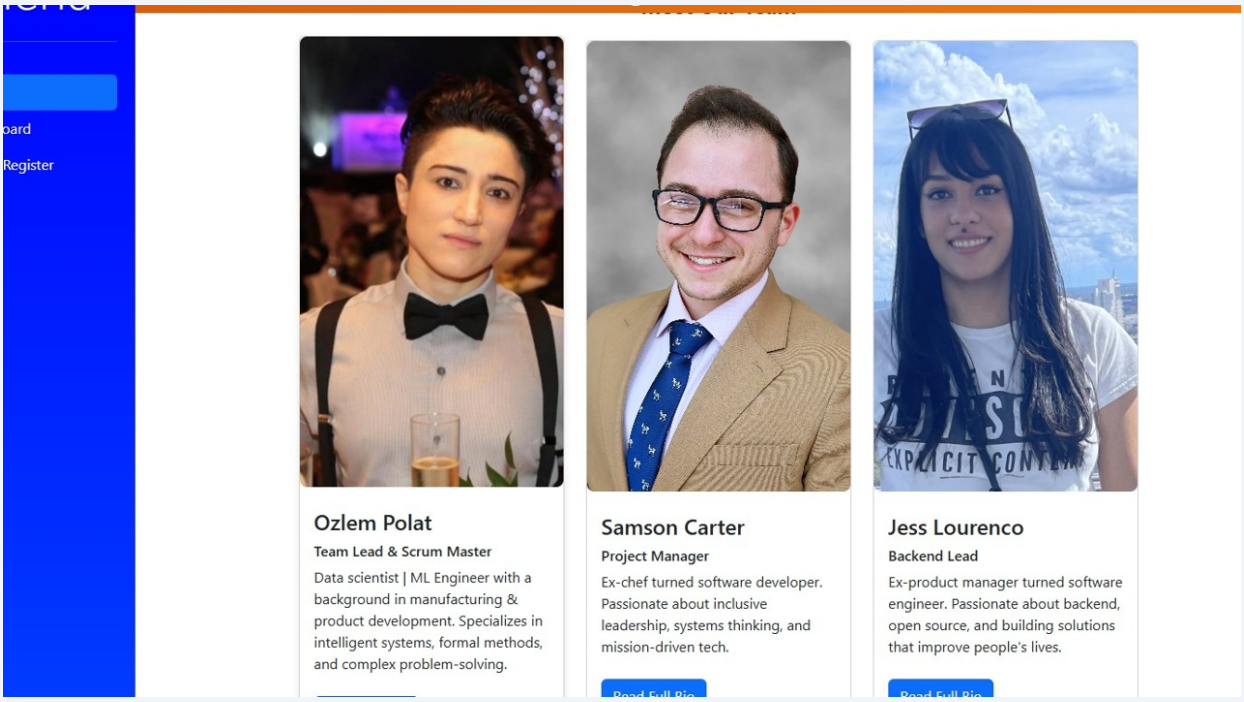
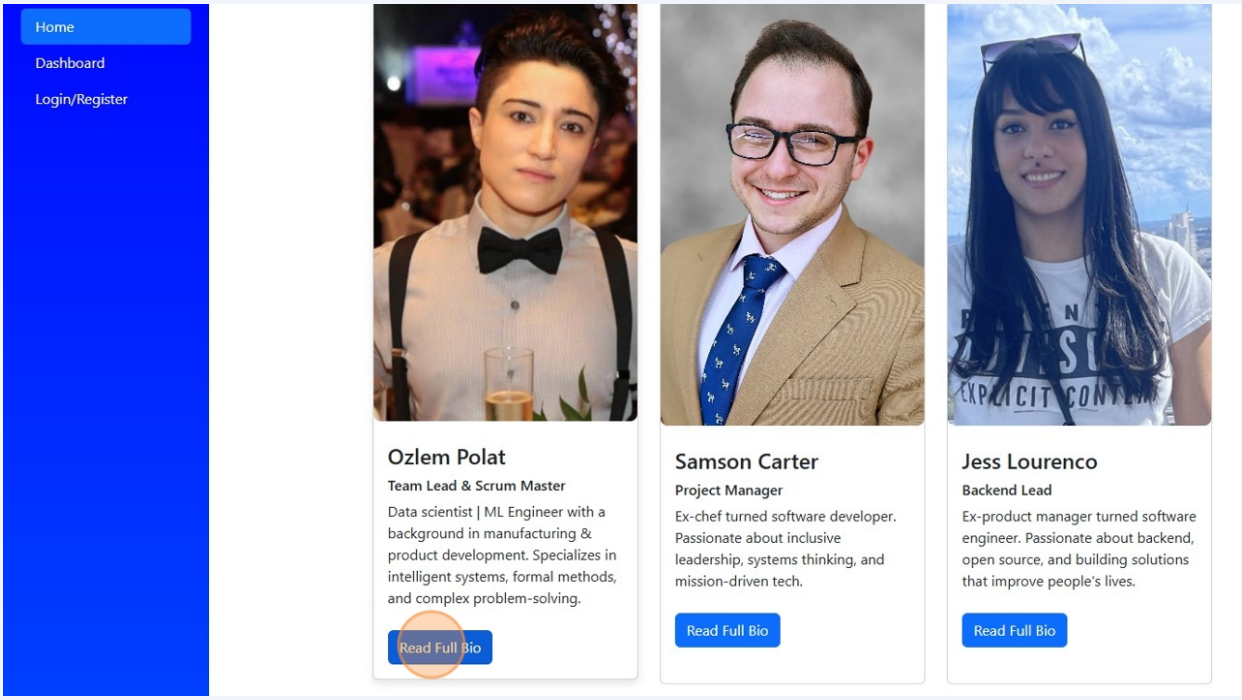
Navigating and Managing System Tables and Graphs

1 To access the application, start the docker container and follow it to the Dash app, hosted at http://127.0.0.1:8000

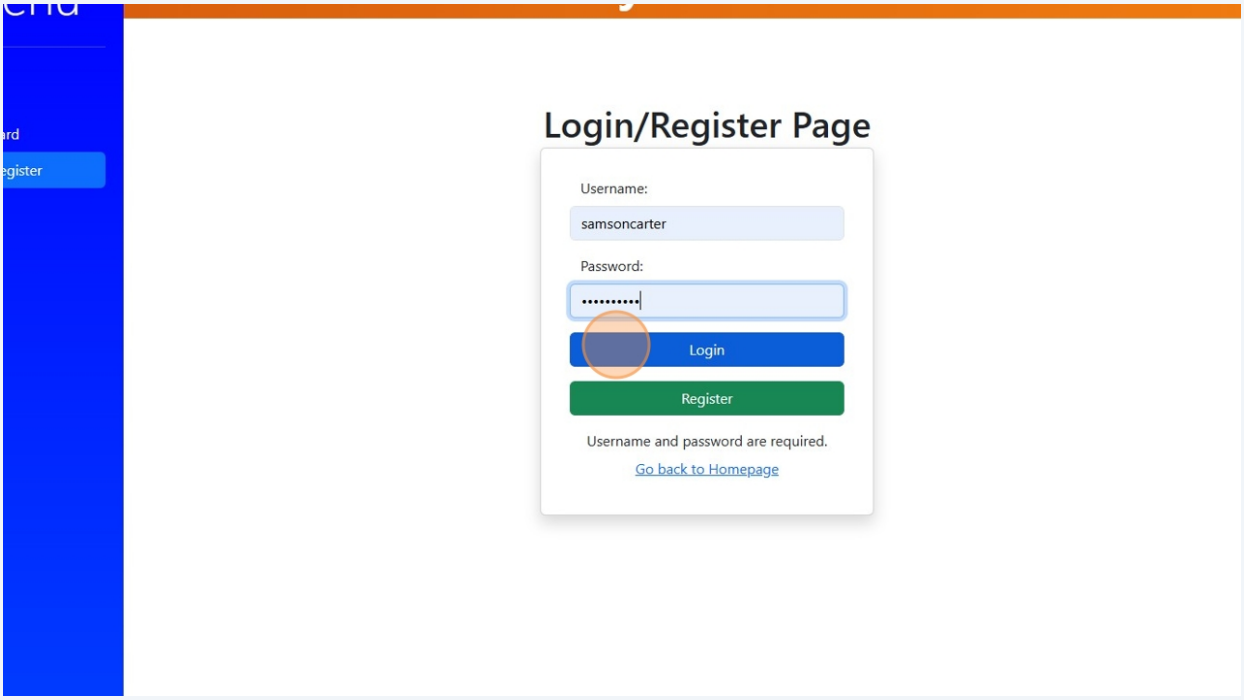


2 From the home page, read the full bio of any of the team members by selecting the "Read Full Bio" button within their introduction card.

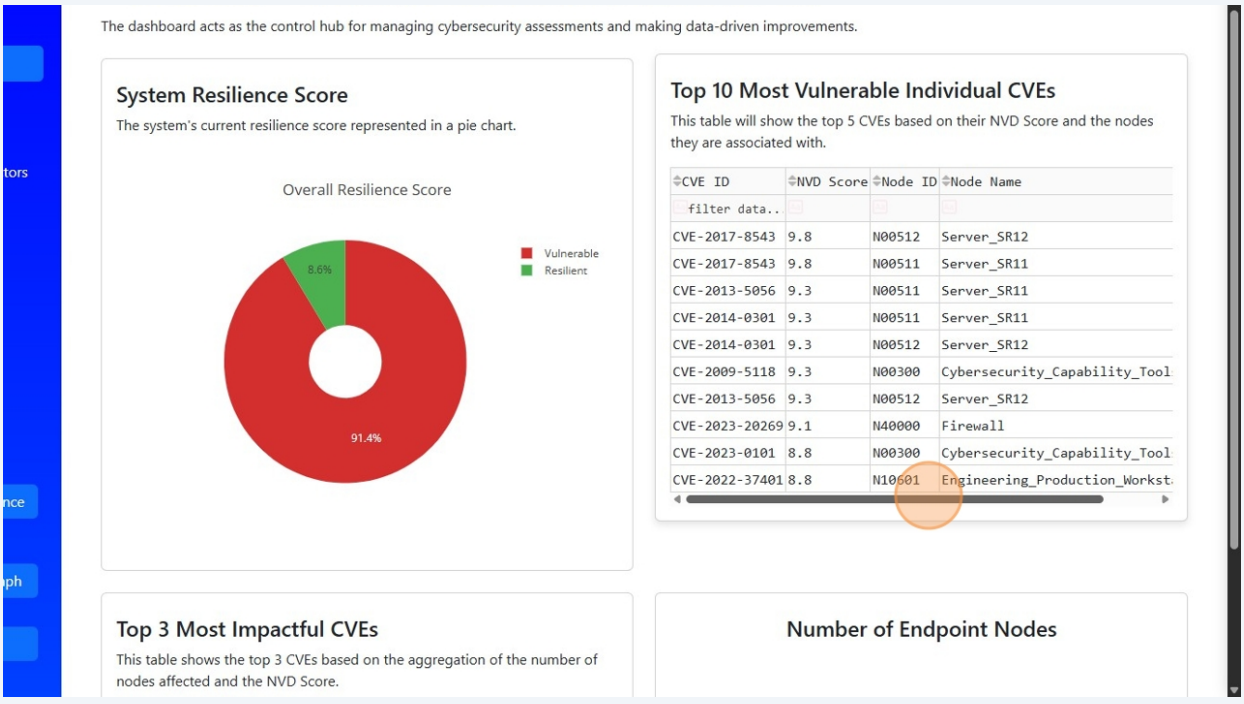


3 To access the full application, Click "Login/Register" on the sidebar

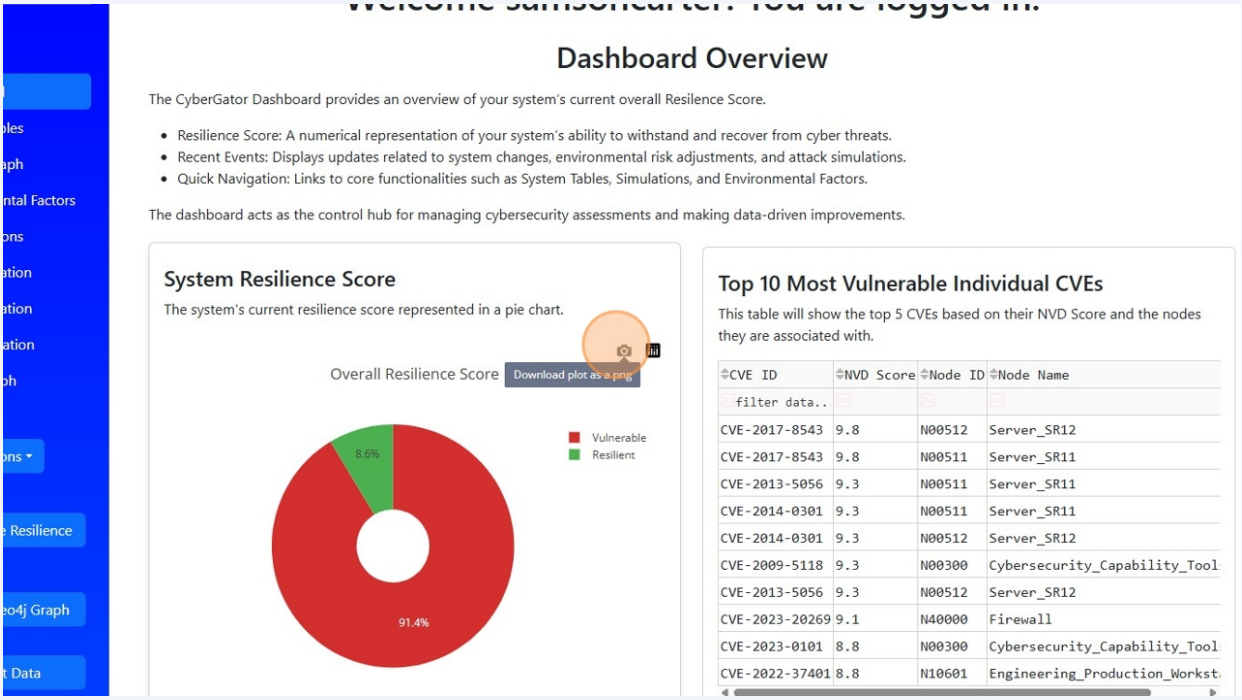
4 To register/log in, enter your unique user name and password and then select either register for new users or log in for existing users



5 After logging in, users are redirected to the dashboard, where the overall score, 10 most vulnerable individual CVEs, Most impactful CVEs and Number of system endpoints are displayed

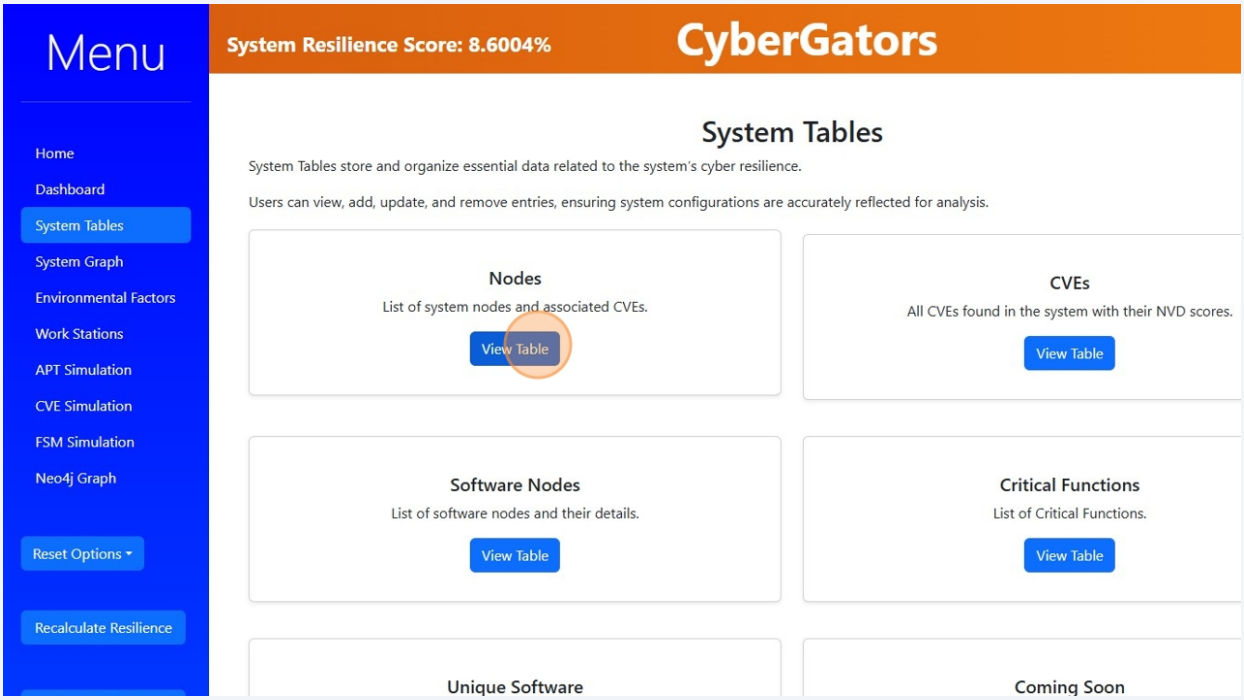


6 To download a static copy of the current System Resilience score, select this button

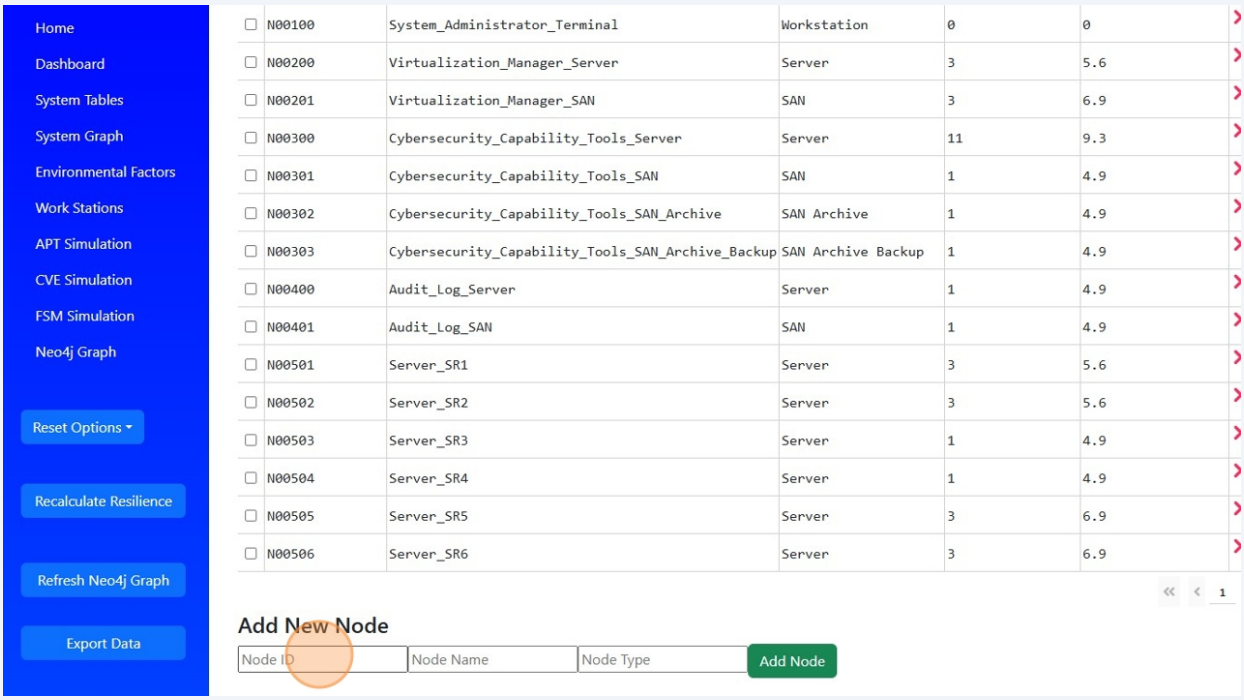


7 Click "System Tables" to view the system tables

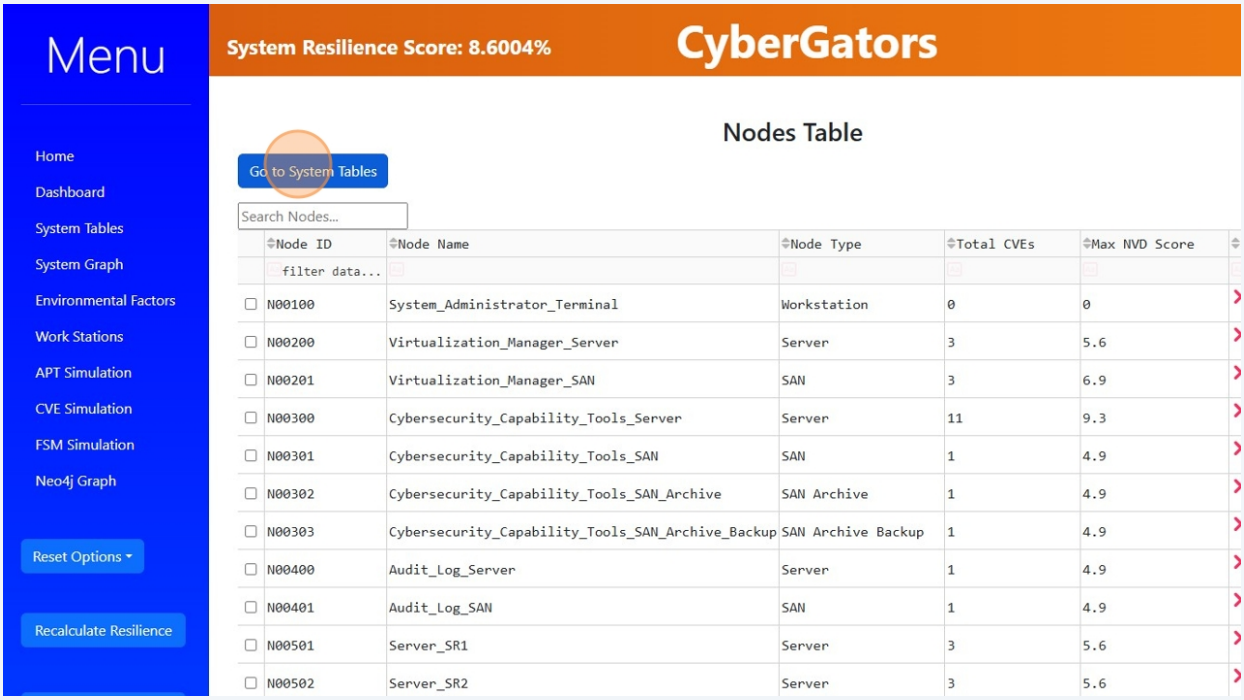
8 To view any of the tables listed, click "View Table"



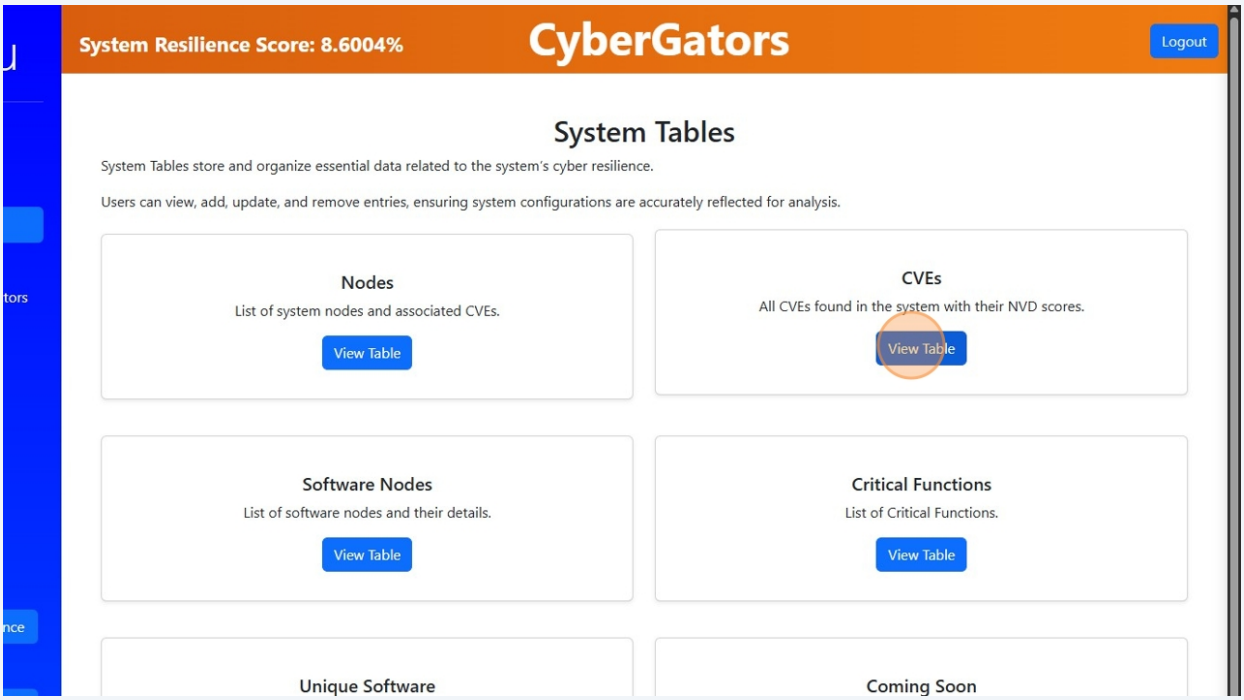
9 The Nodes table is a comprehensive list of all the nodes within the system. To add a node, Add a nodeID, Node Name, and Node type, and then select Add Node



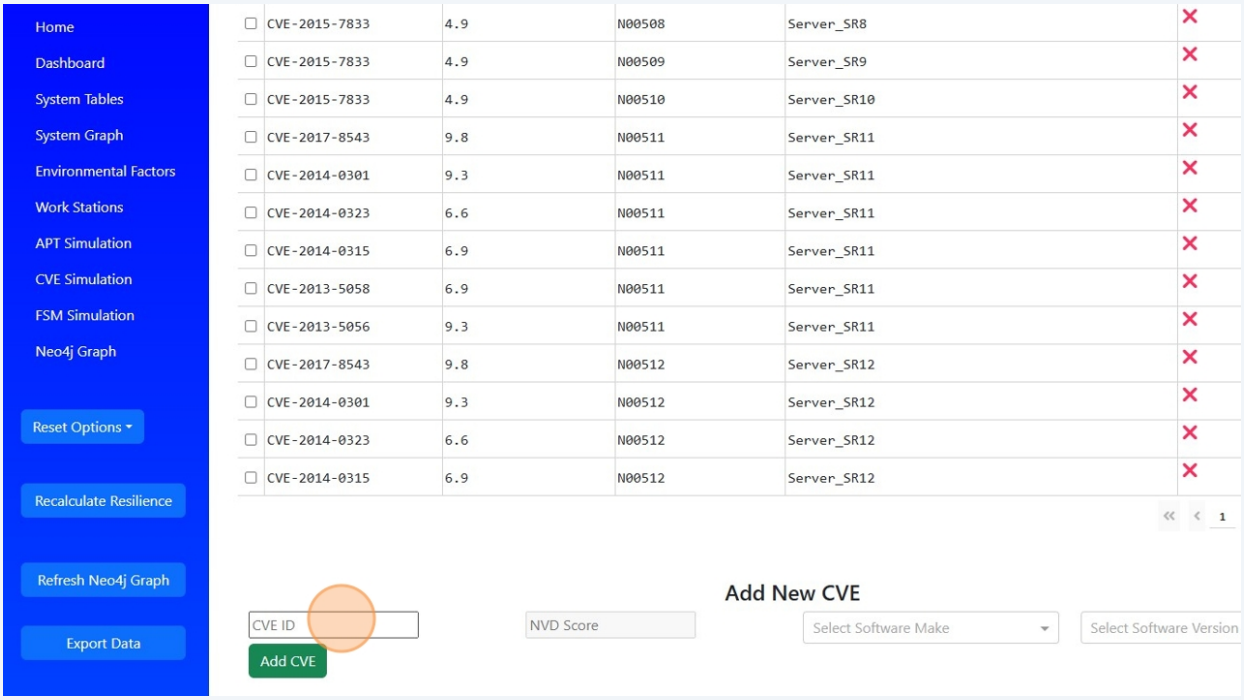
10 To return to the Systems Tables at any time, click "Go to System Tables"



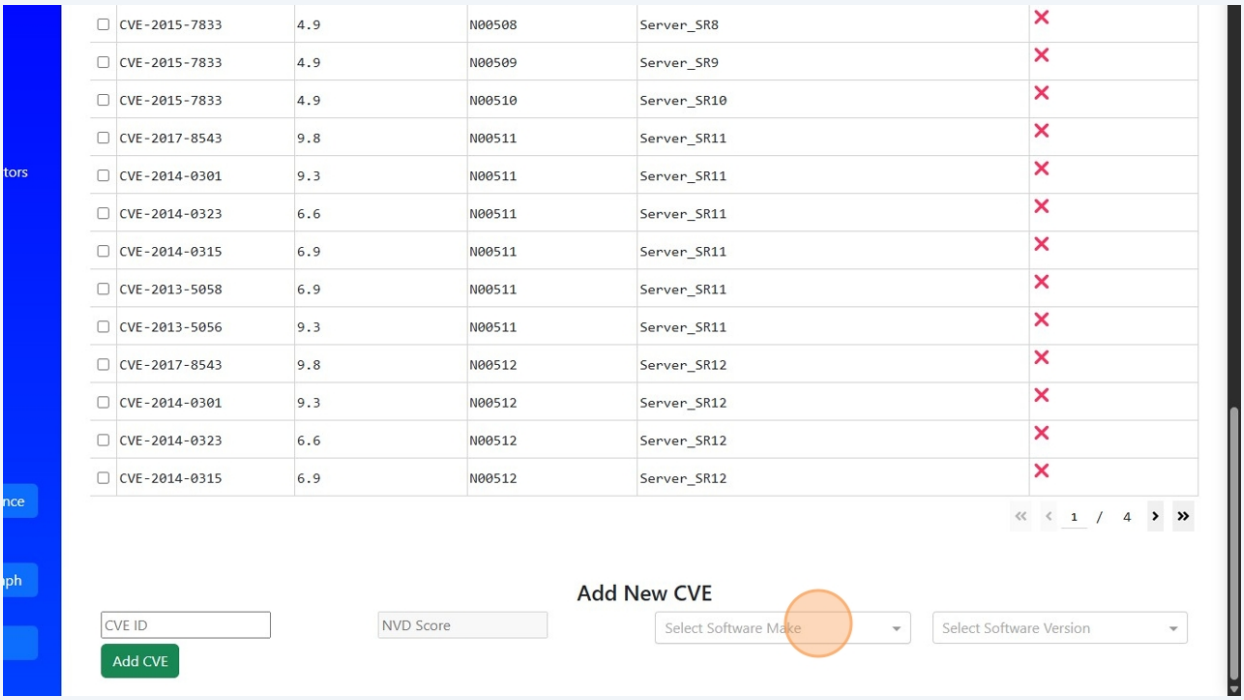
11 Next, let's view the CVE table, a comprehensive list of all CVEs in the system and the nodes they are associated with



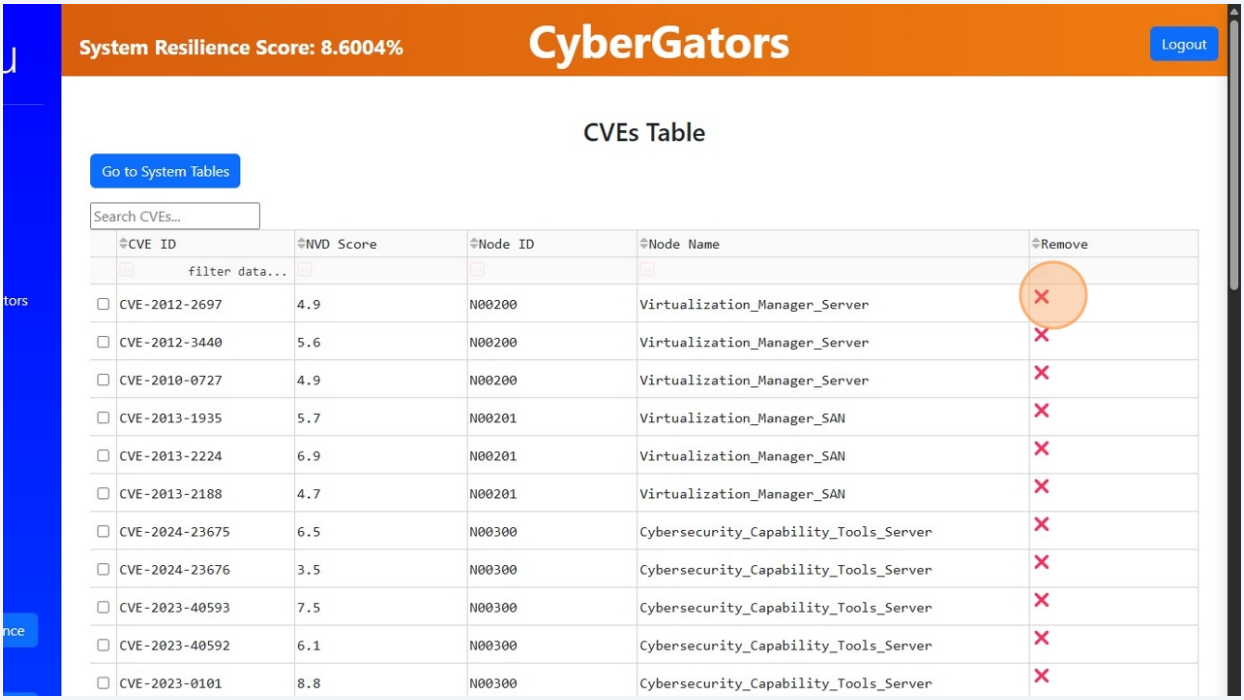
12 To add a CVE, Click the "CVE ID" field. Once the CVE has been added, the NVD score will be automatically called through the MITRE TAXI API.



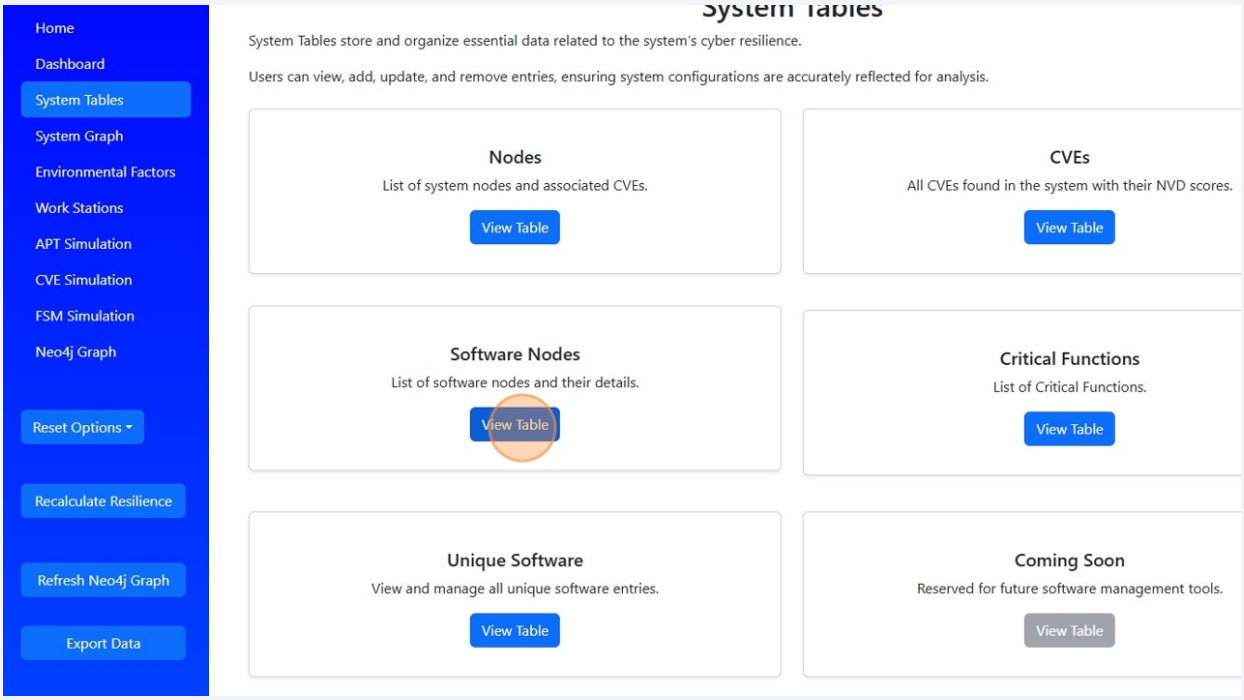
13 Select the software make and version that it implicates, then click "Add CVE"



14 To remove a single CVE from a particular node, Click the Remove "" Button

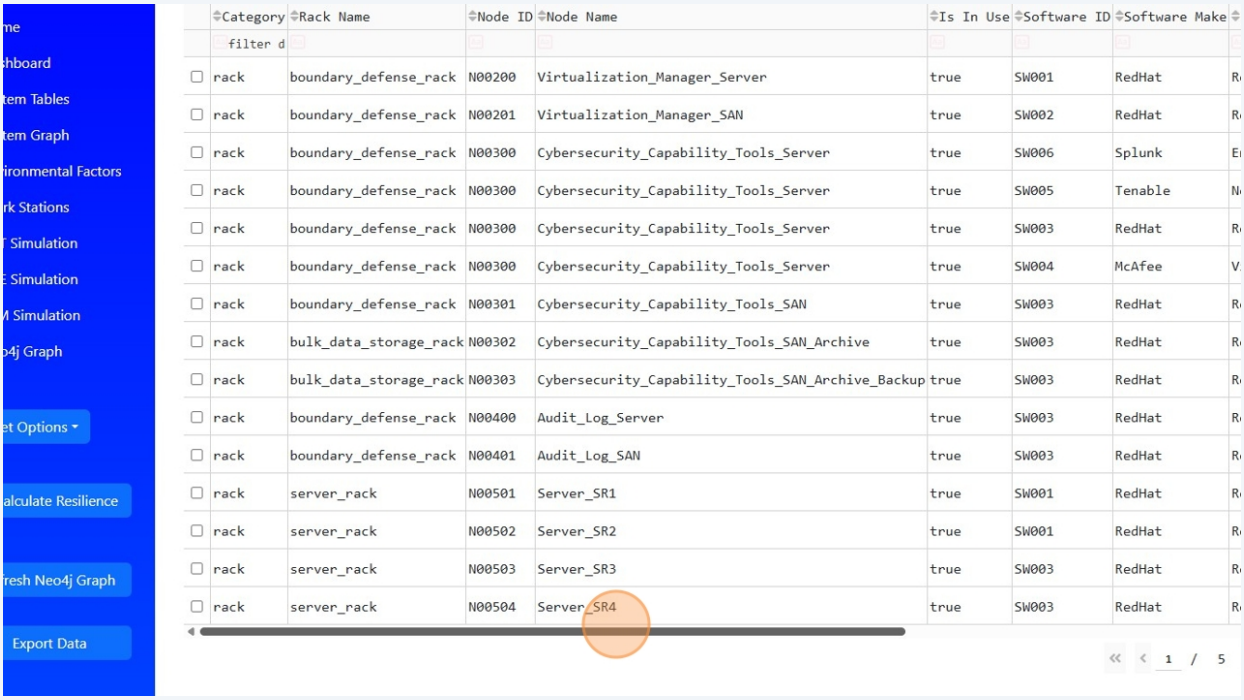


15 To view the Software Nodes, click "View Table" underneath the Software Nodes card in the System Tables page.



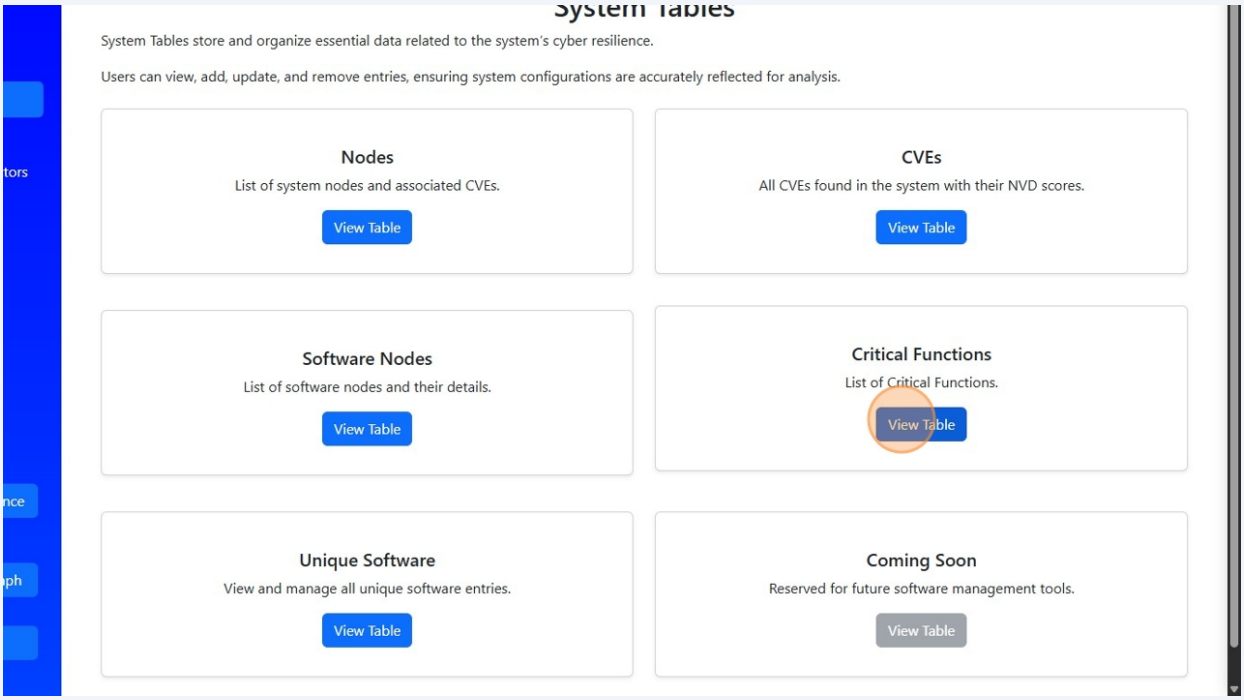
16

The software Nodes shows all the software within the system as well as the nodes where the software is hosted.



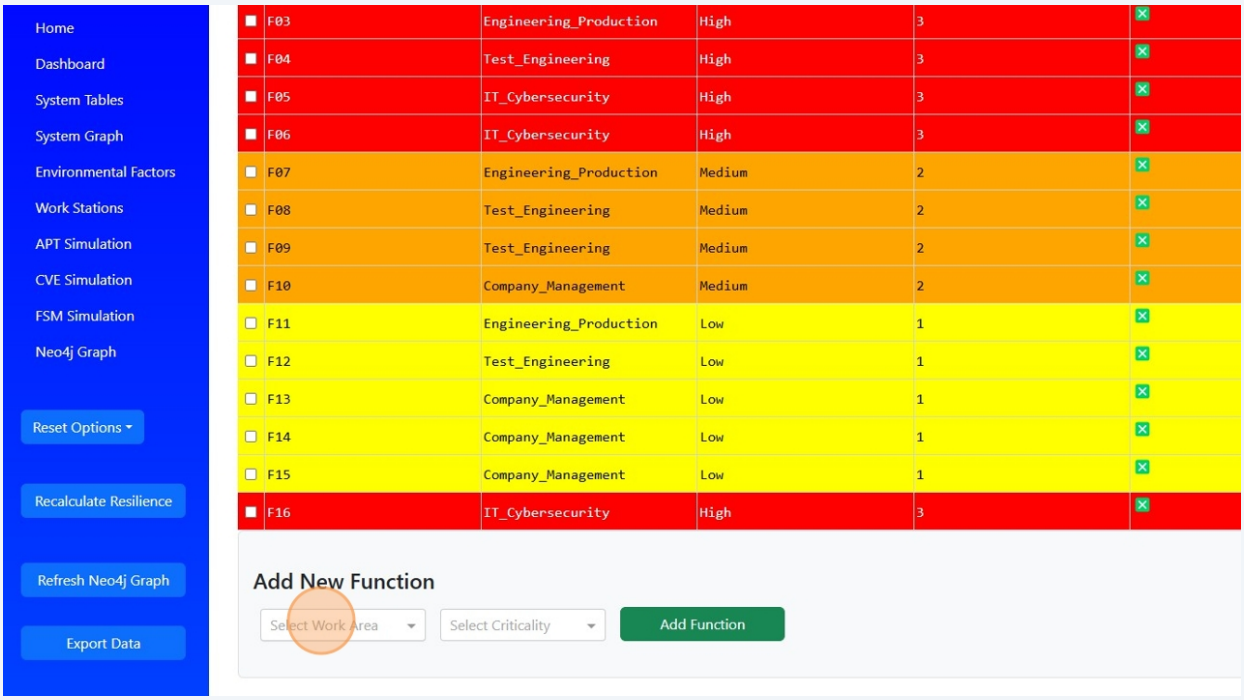
17

To view the Critical Functions within the system, select "View Table" in the Critical Functions tile on the System Tables page.

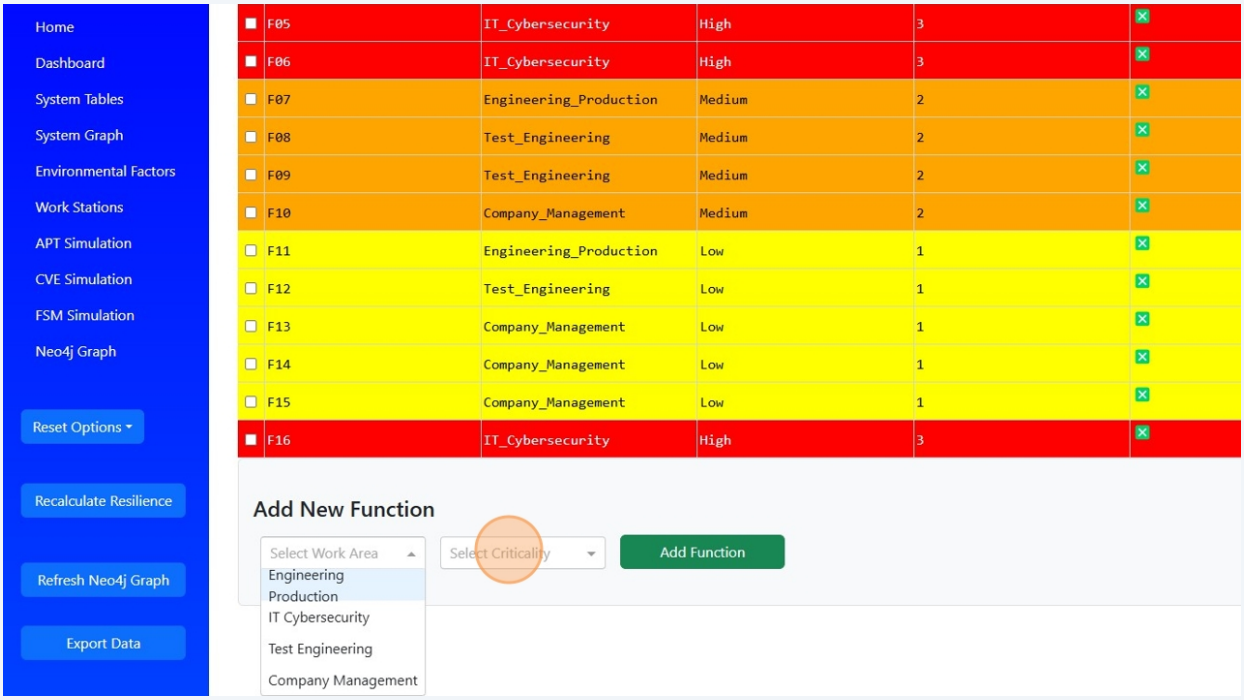


18 To remove a Critical Function from the system, Click "□"

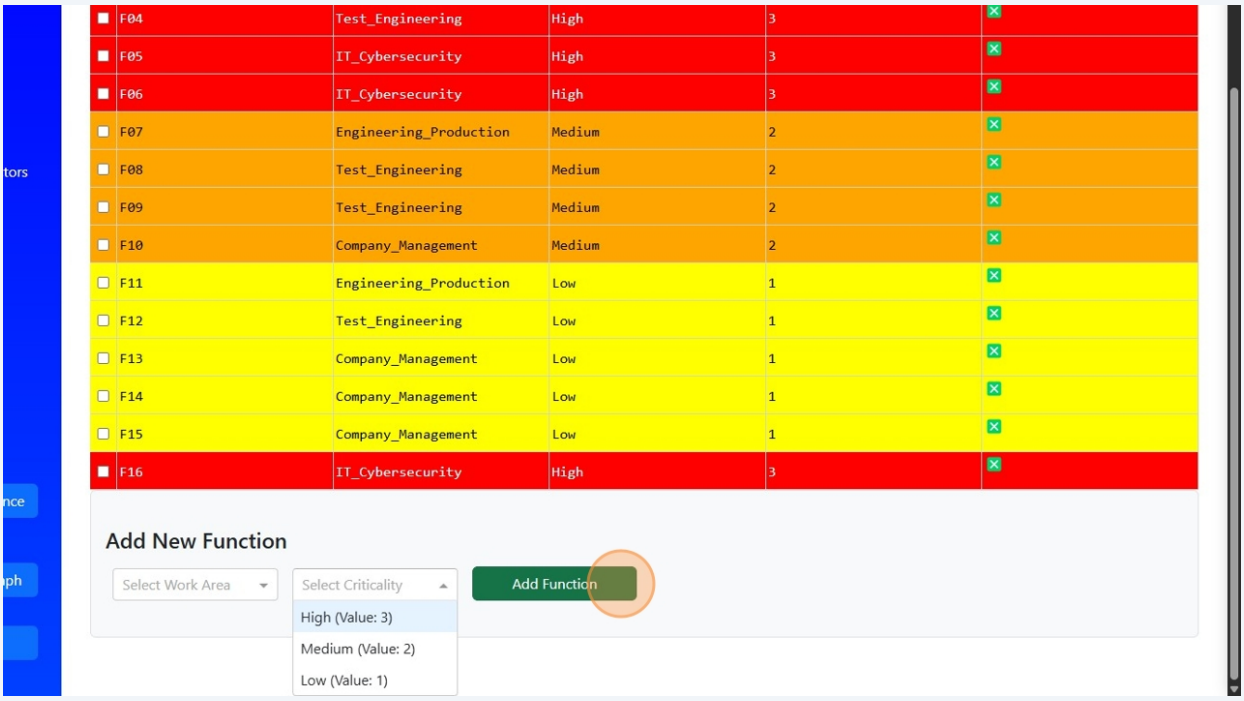
19 To add a new Critical Function, Click "Select Work Area" and select the work area.



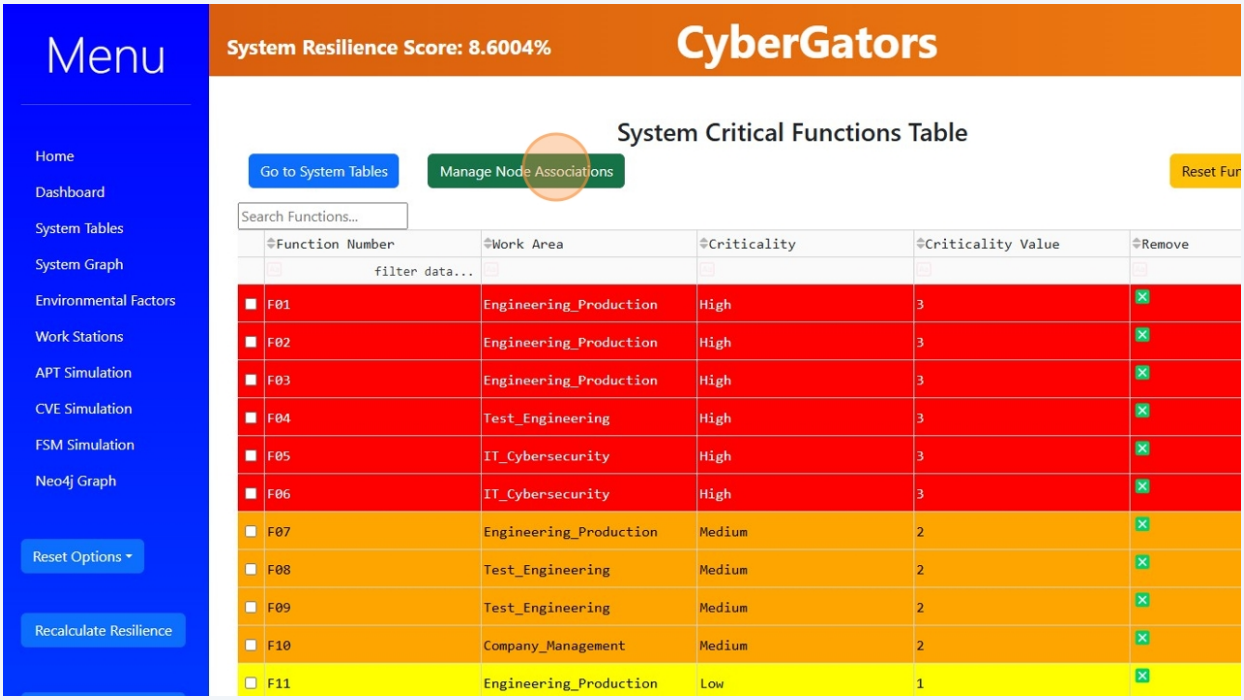
20 Next, click "Select Criticality" and set the criticality level.



21 To add it to the system, click "Add Function"

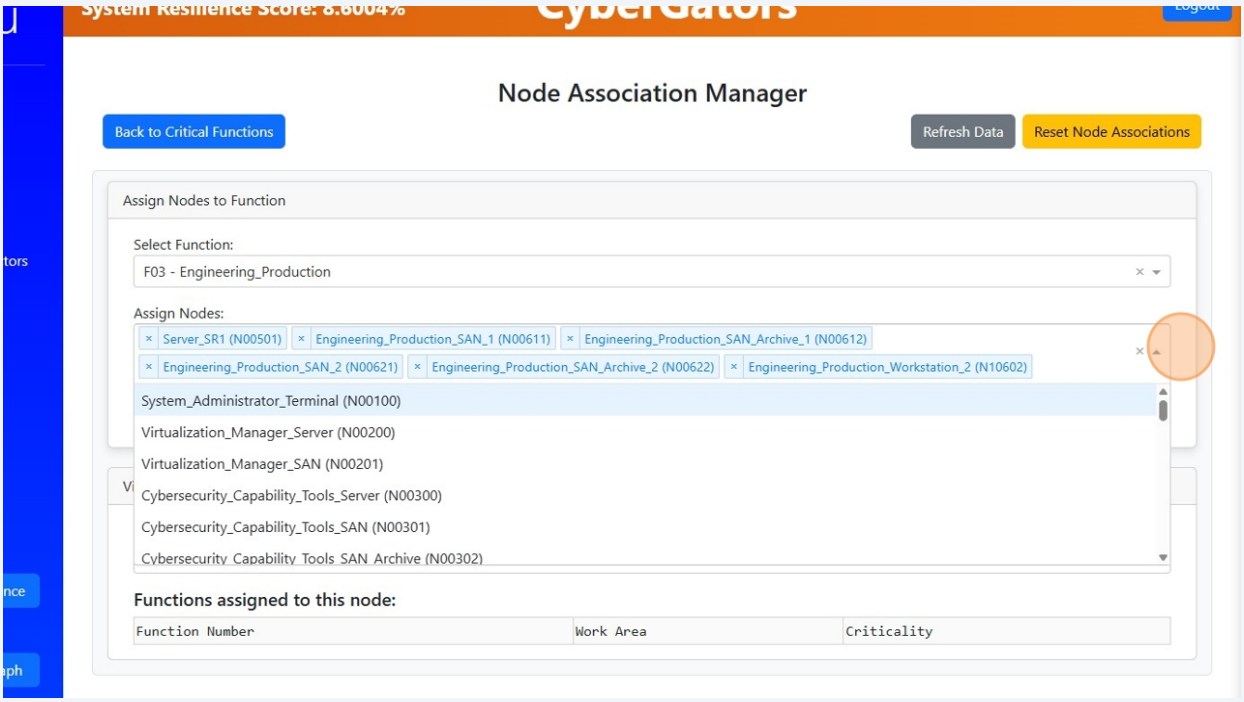


22 To view the nodes the are associated with the various critical functions, click "Manage Node Associations"

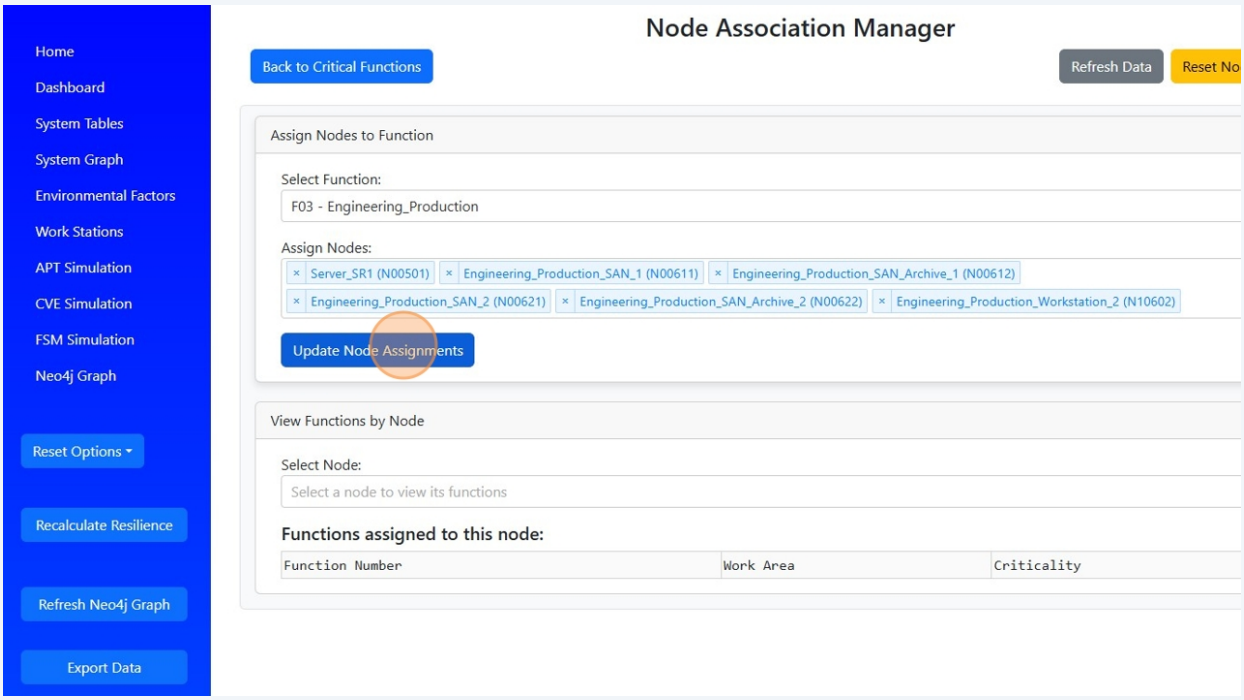


23 To assign nodes to a function, click "Select a function" and select the function in question.

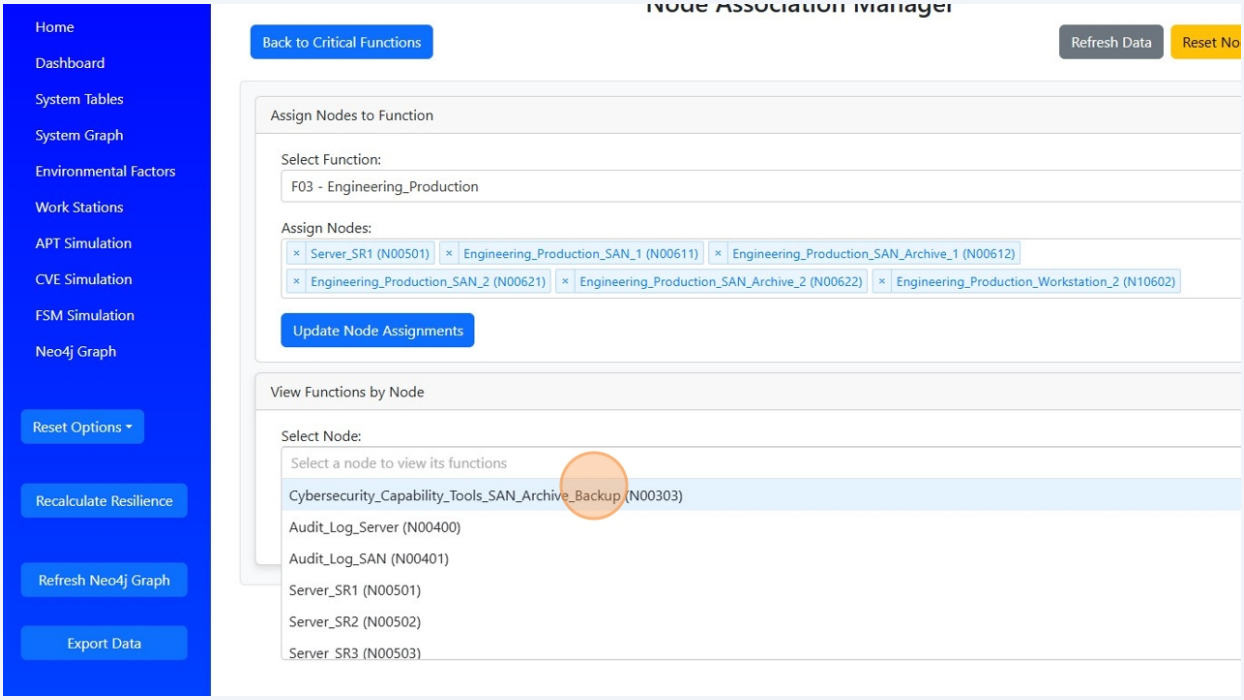
24 Next, view the assigned nodes and add/remove nodes from the list in the Assigned Nodes block.



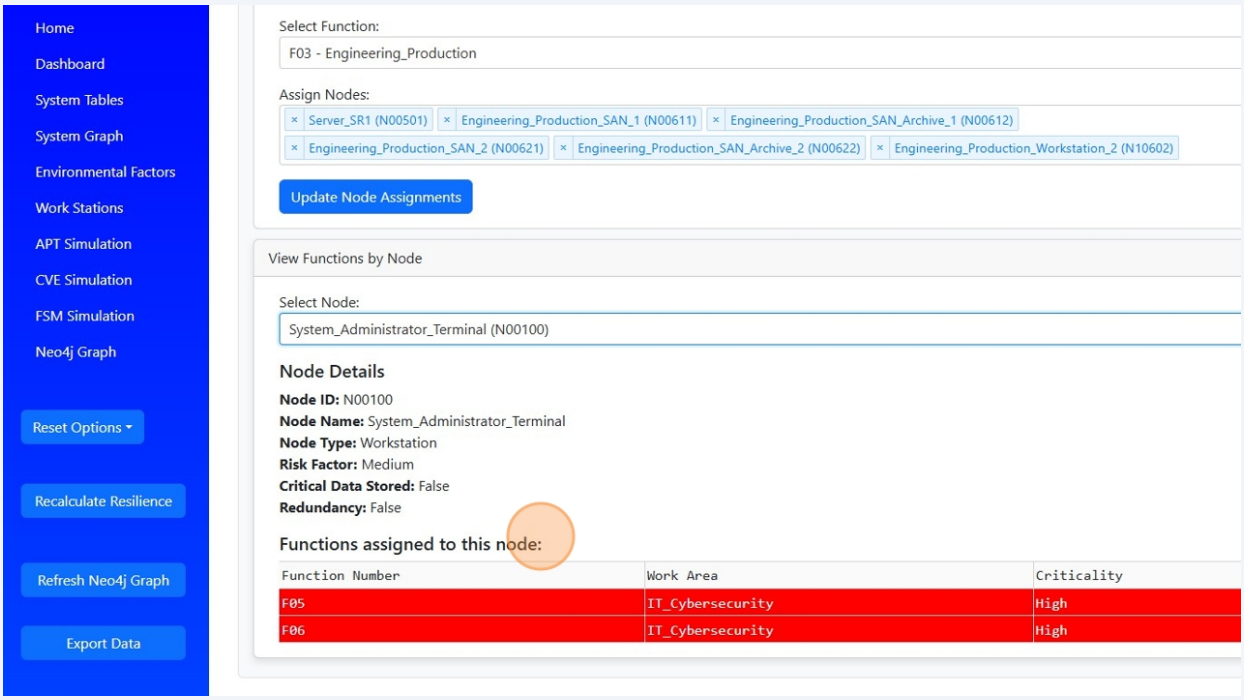
25 Click "Update Node Assignments"



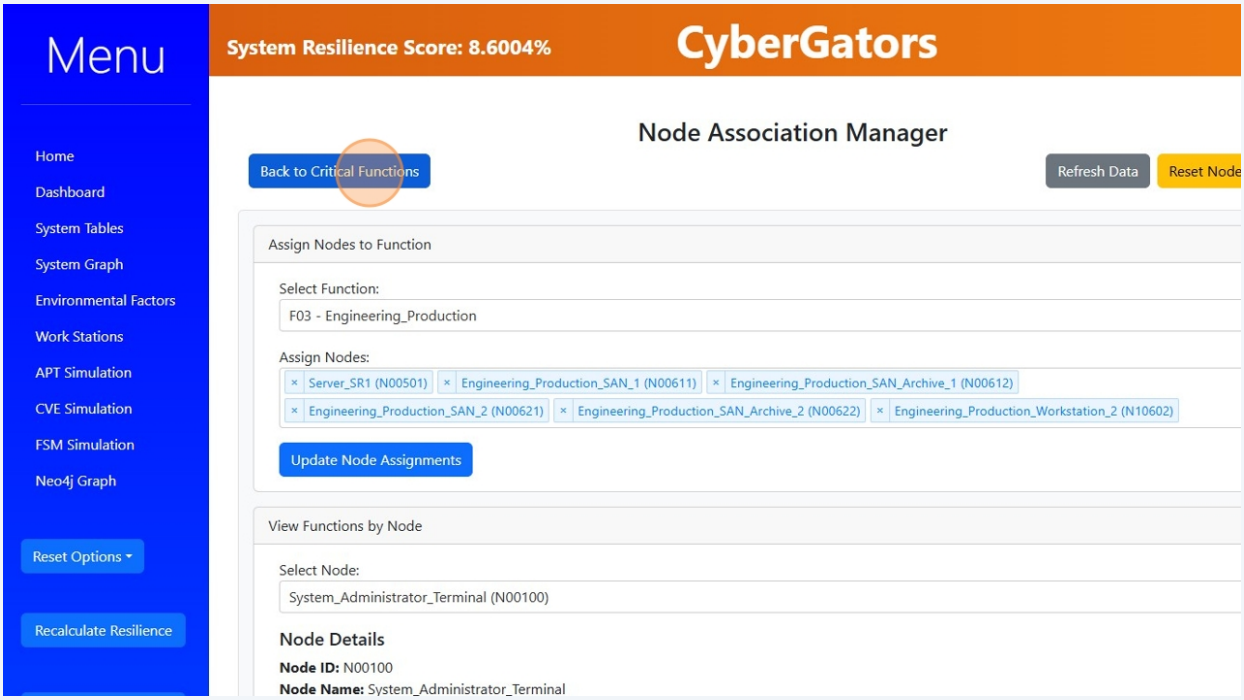
26 To view the functions by node, click the dropdown in the View Functions by Node block and select a node.



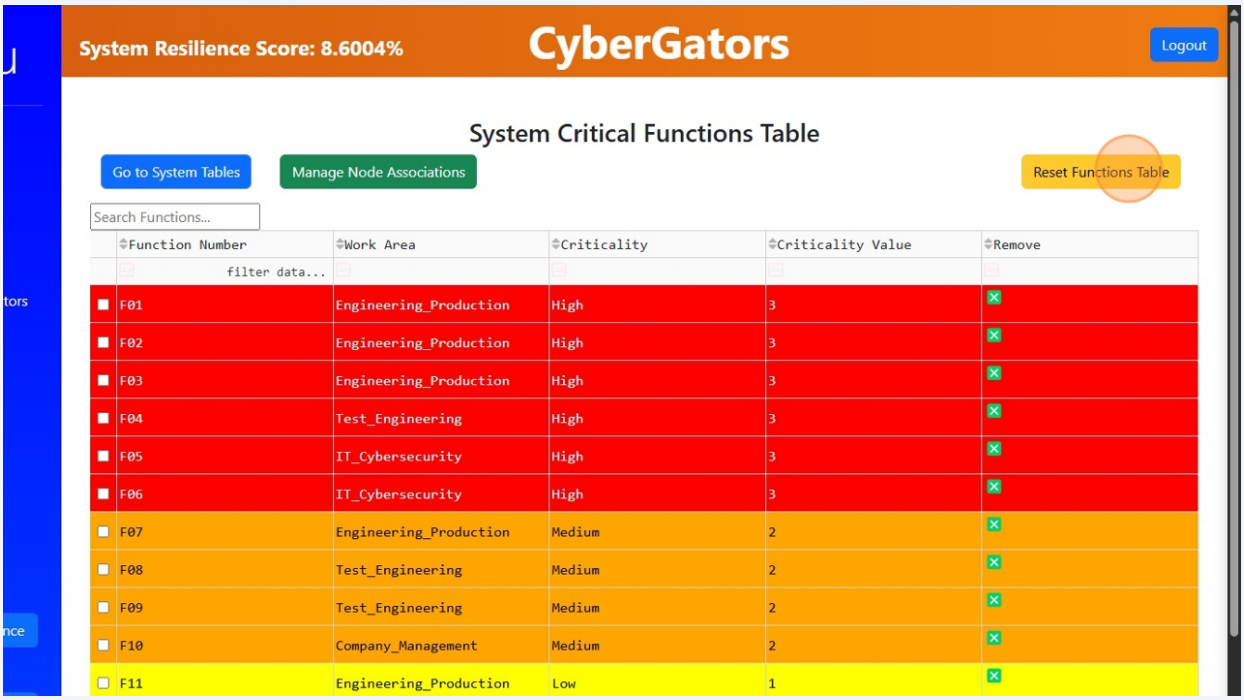
27 Scroll down to view the Functions assigned to a given node, as well as some additional node information.



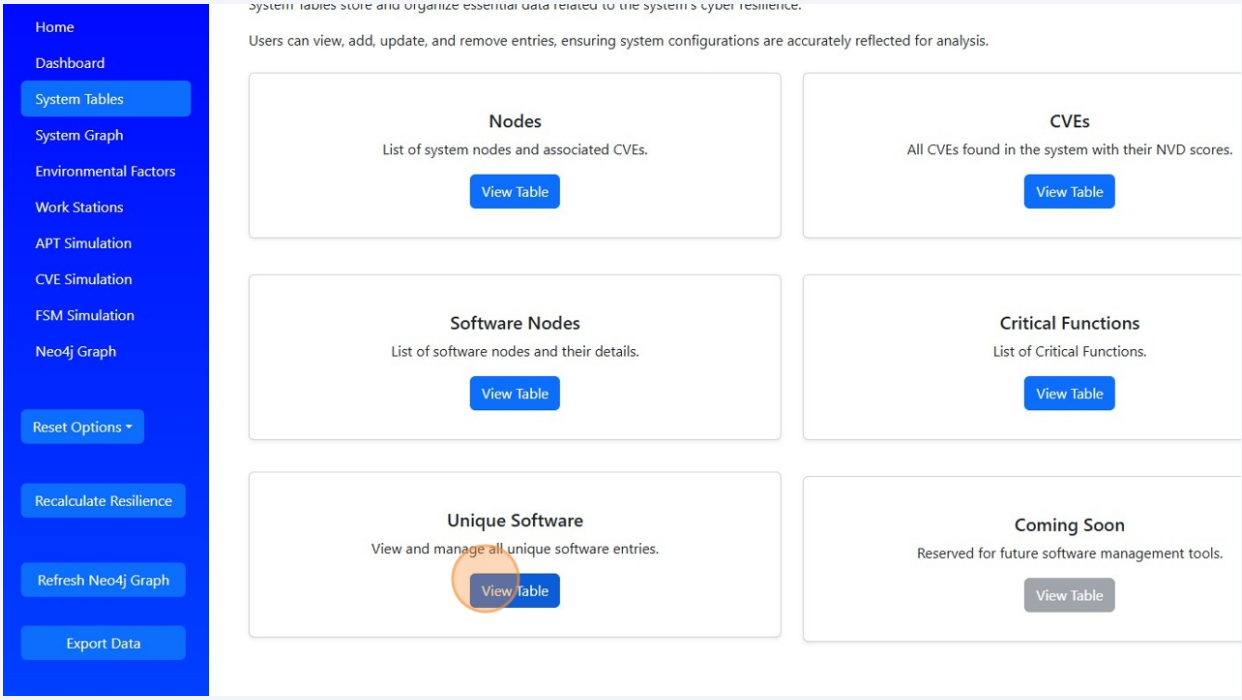
28 To return to the Critical Functions table, click "Back to Critical Functions"



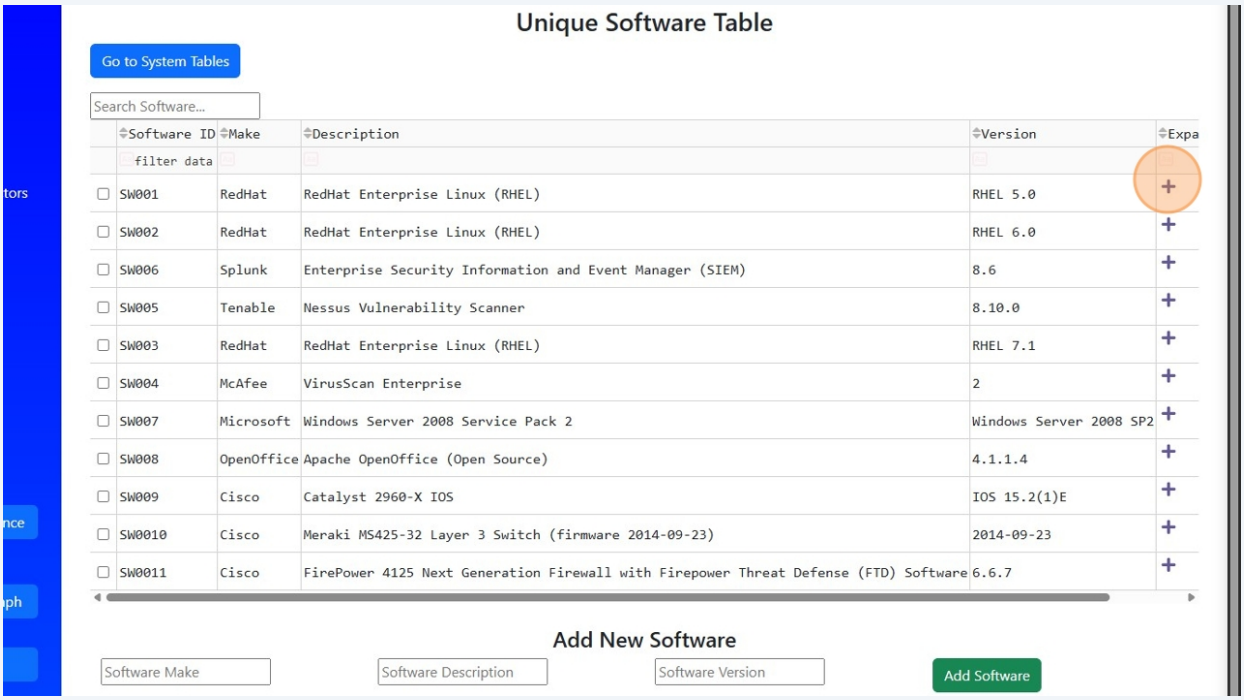
29 To reset the Critical Functions table, Click "Reset Functions Table"



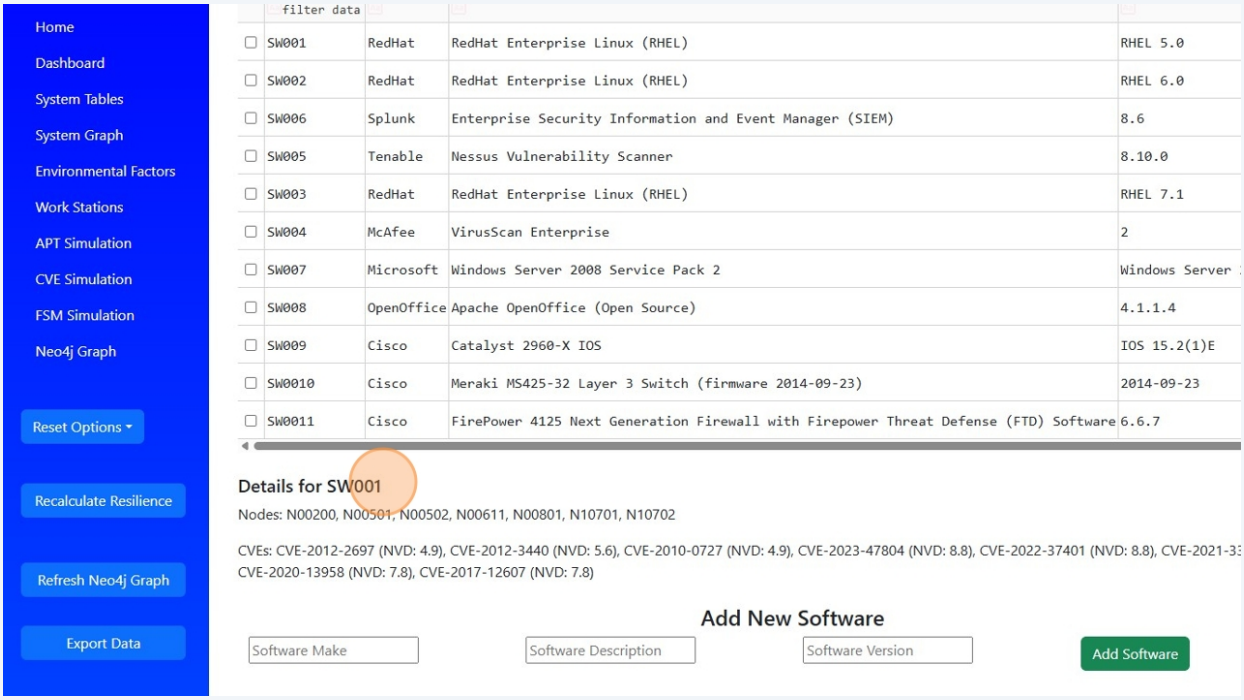
30 To view the Unique Software within the system, click "View Table" within the unique Software card on the System Tables page.



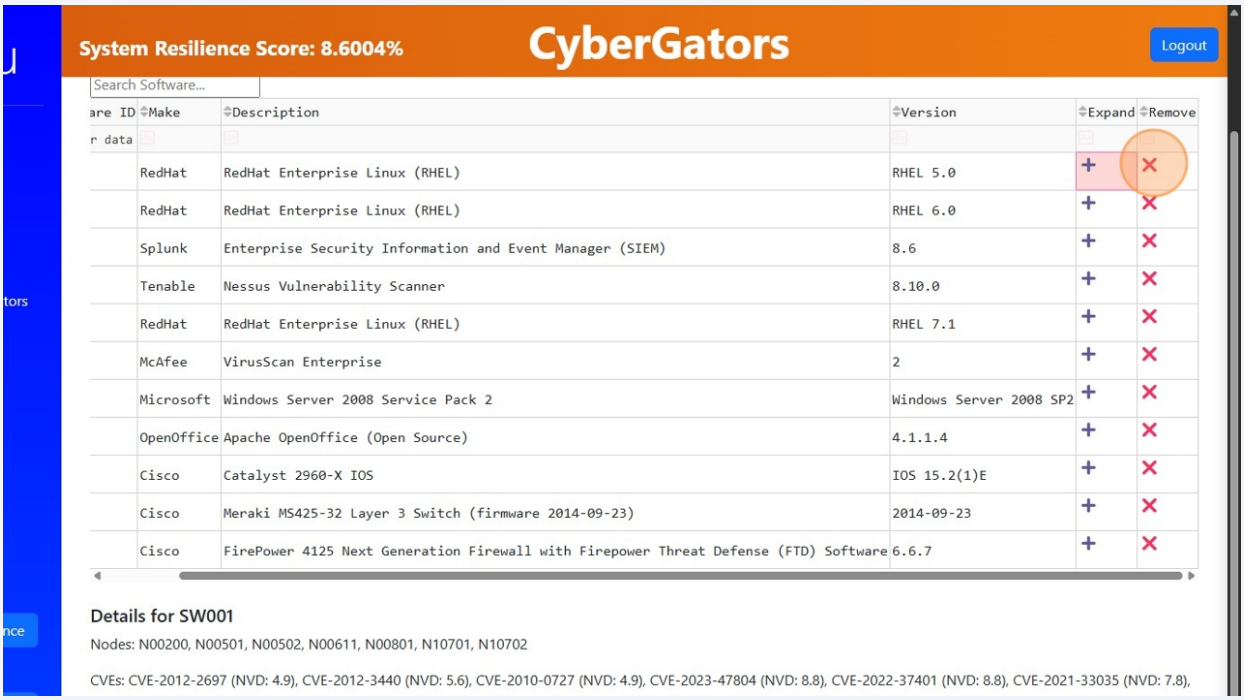
31 The Unique Software Table shows a list of Software, it's makes, their IDs and software versions in a table. Click the "+" to view the details of the software



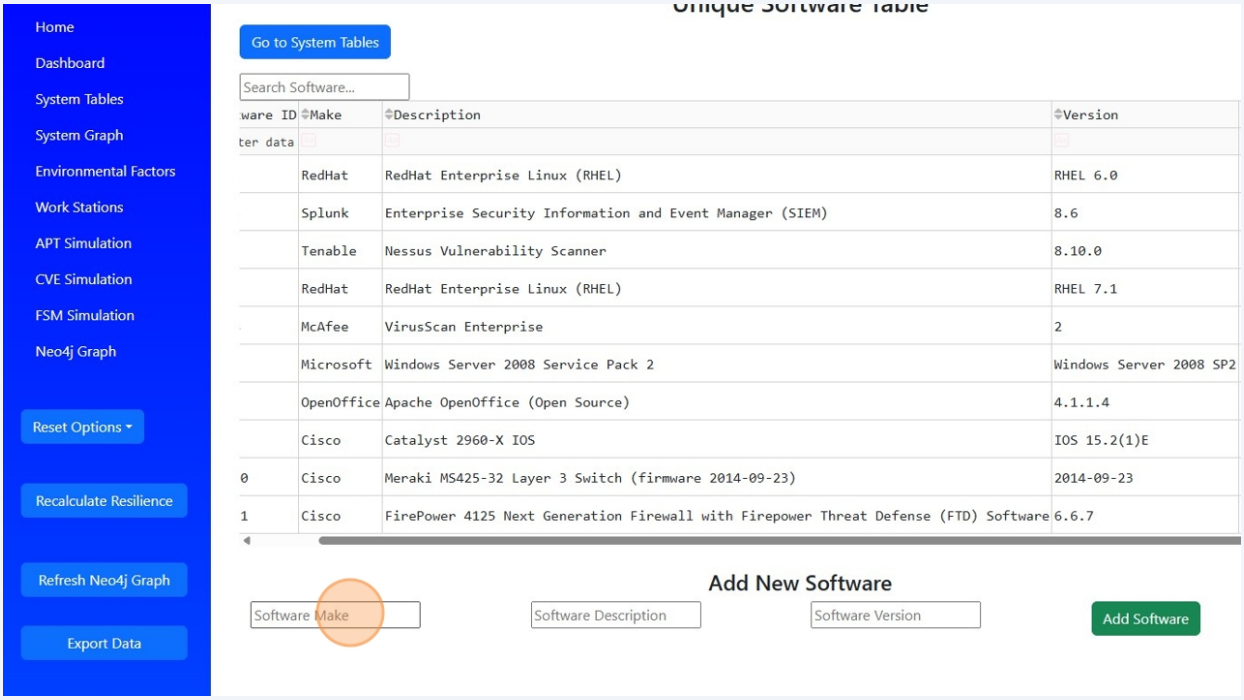
32 The software details show the implicated nodes and currently unpatched CVEs affecting the software.



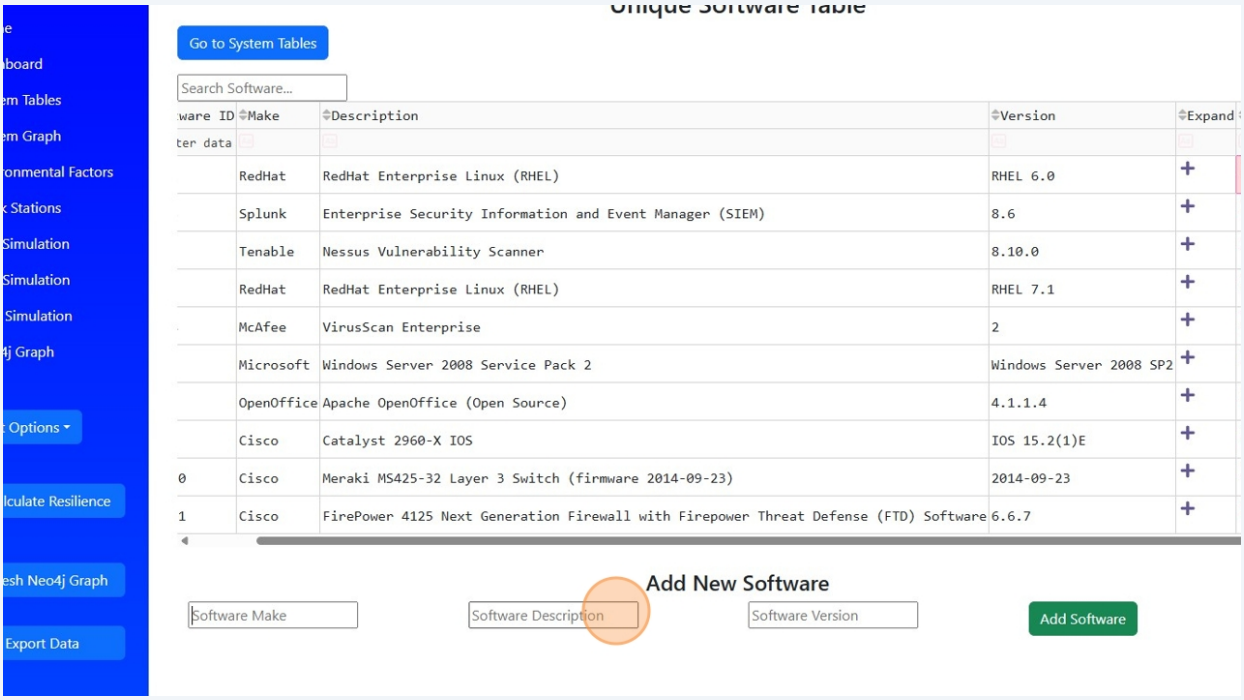
33 To remove the Software from the system, click "□"



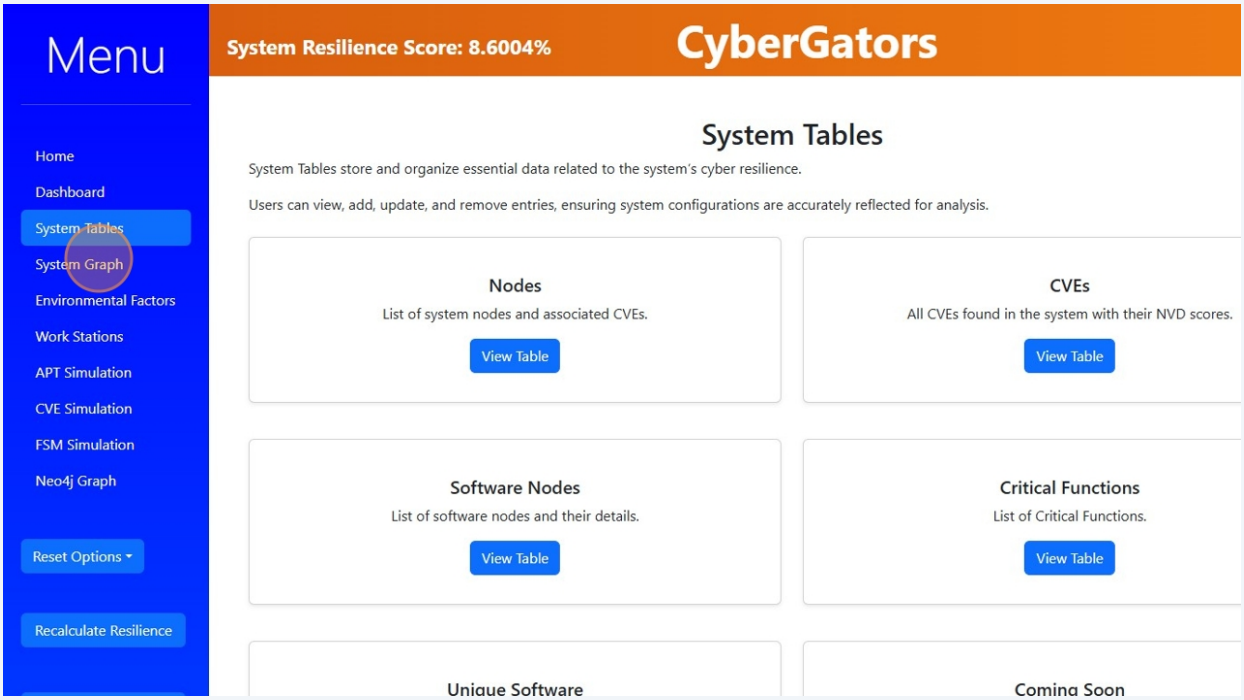
34 To add a new software to the system, click the "Software Make" field. and type in the Make



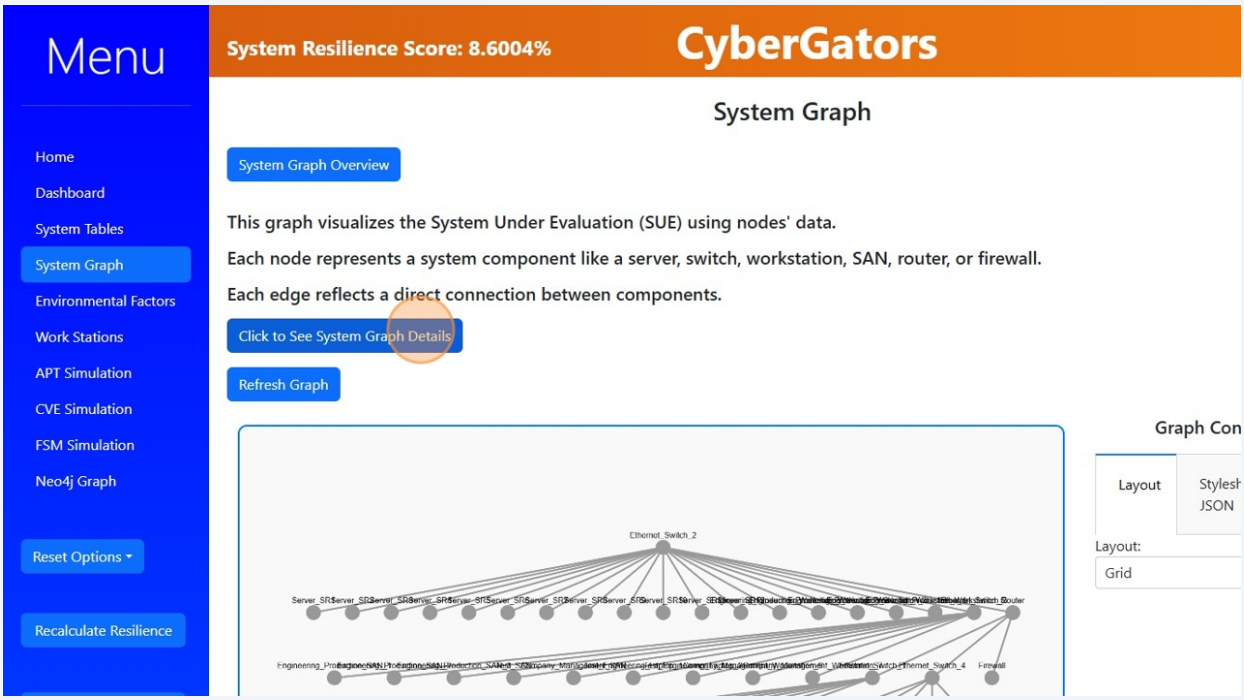
35 Next, add the software description and version, then hit the "Add Software" button.



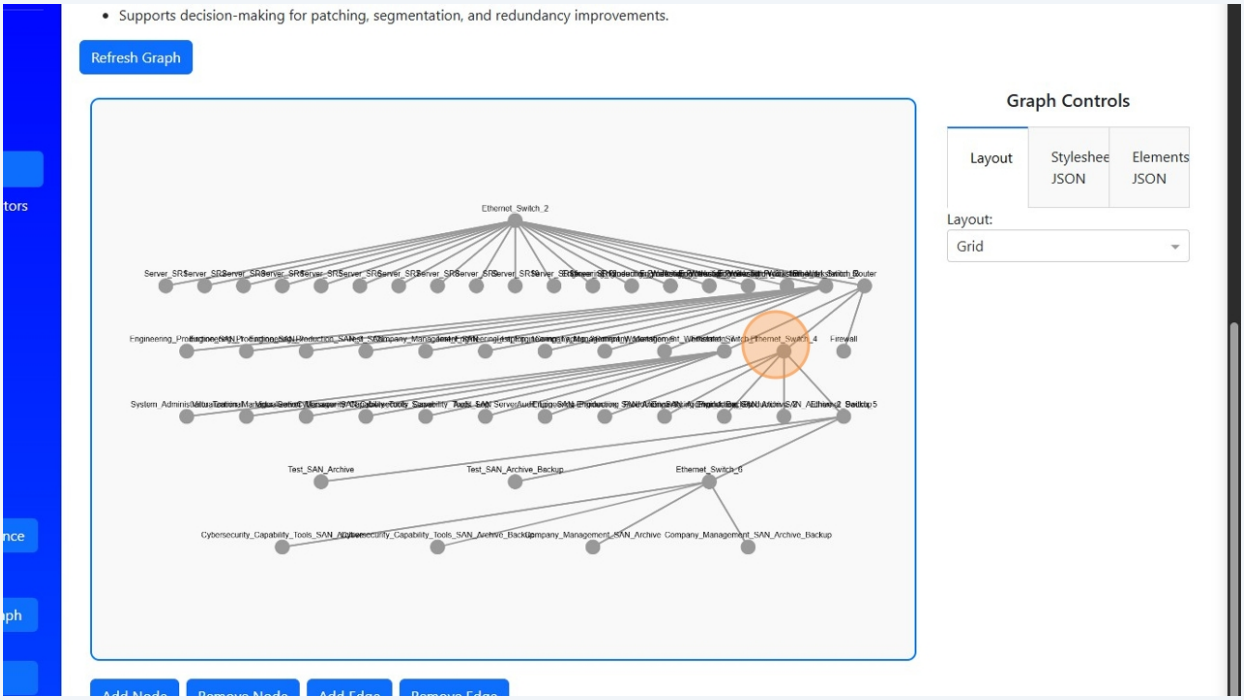
36 Next, let's explore the system graph table. Click "System Graph" on the sidebar.



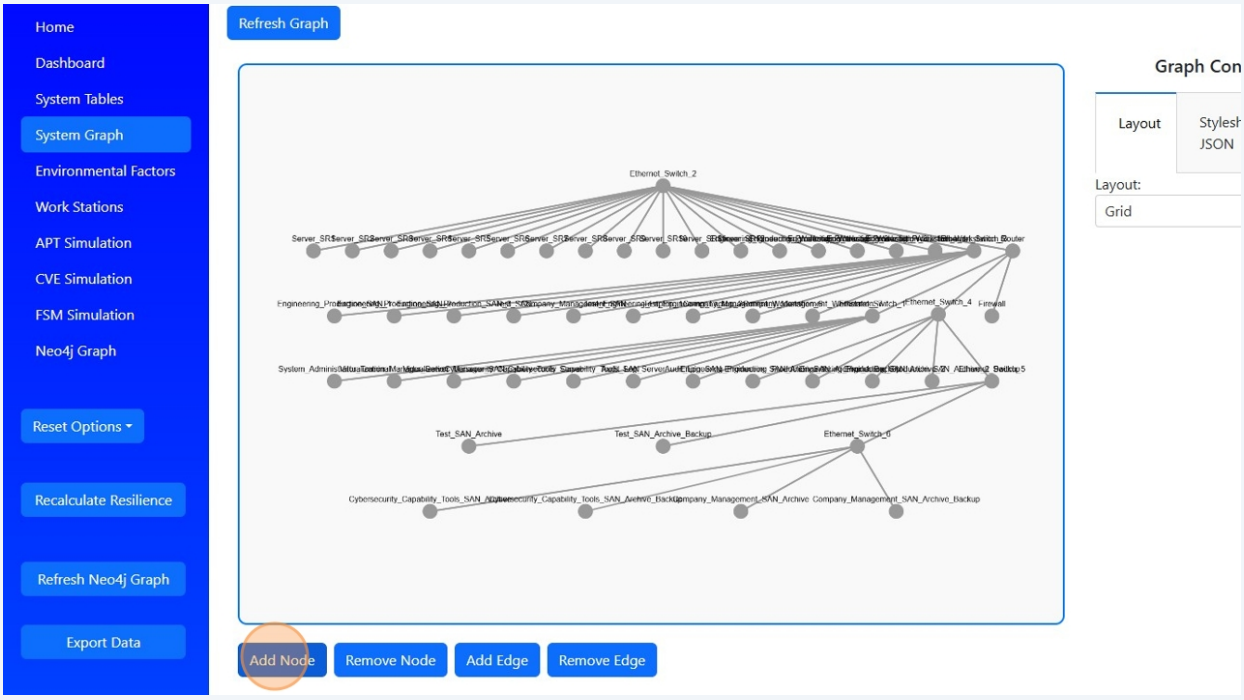
37 To learn more about the system graph and what it means, click "Click to See System Graph Details"



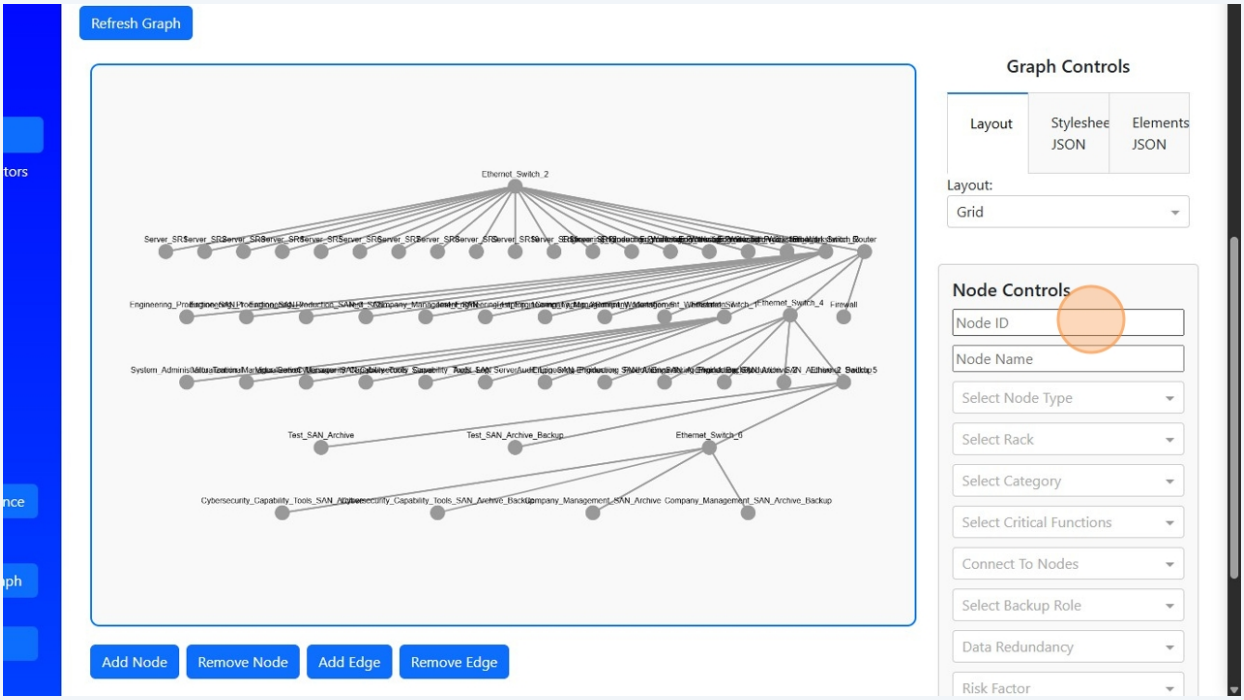
38 Select a node within the graph by clicking on it.



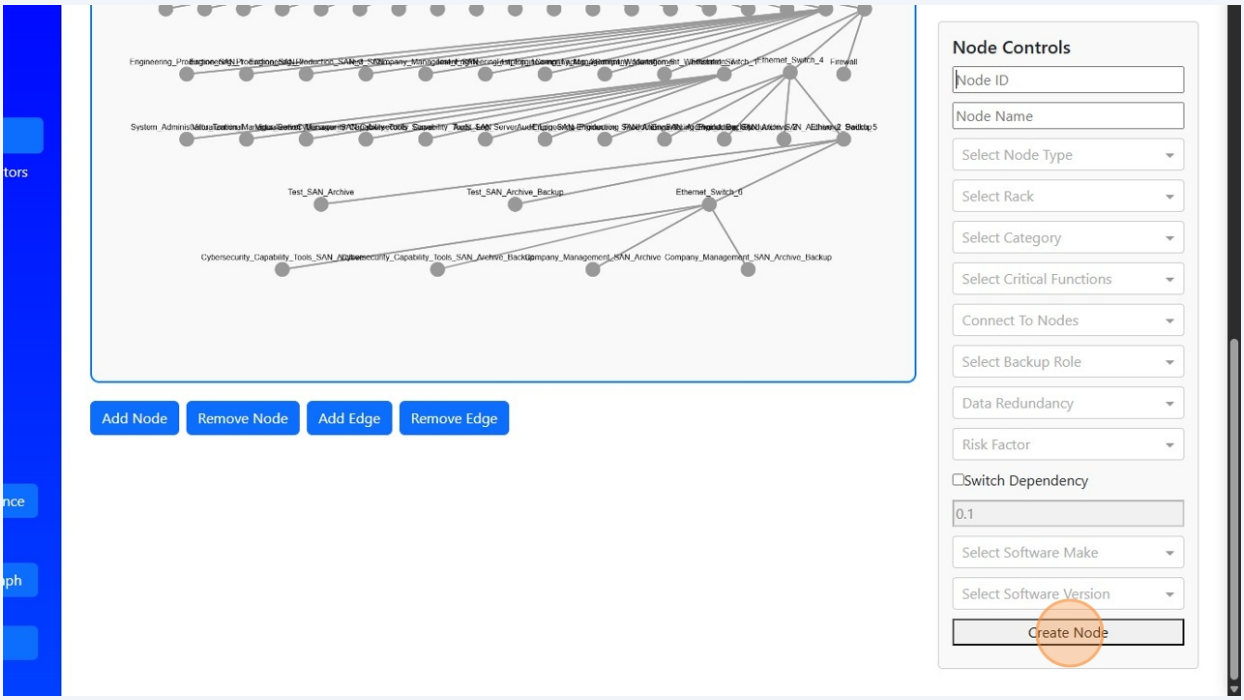
39 To add a node, click "Add Node"



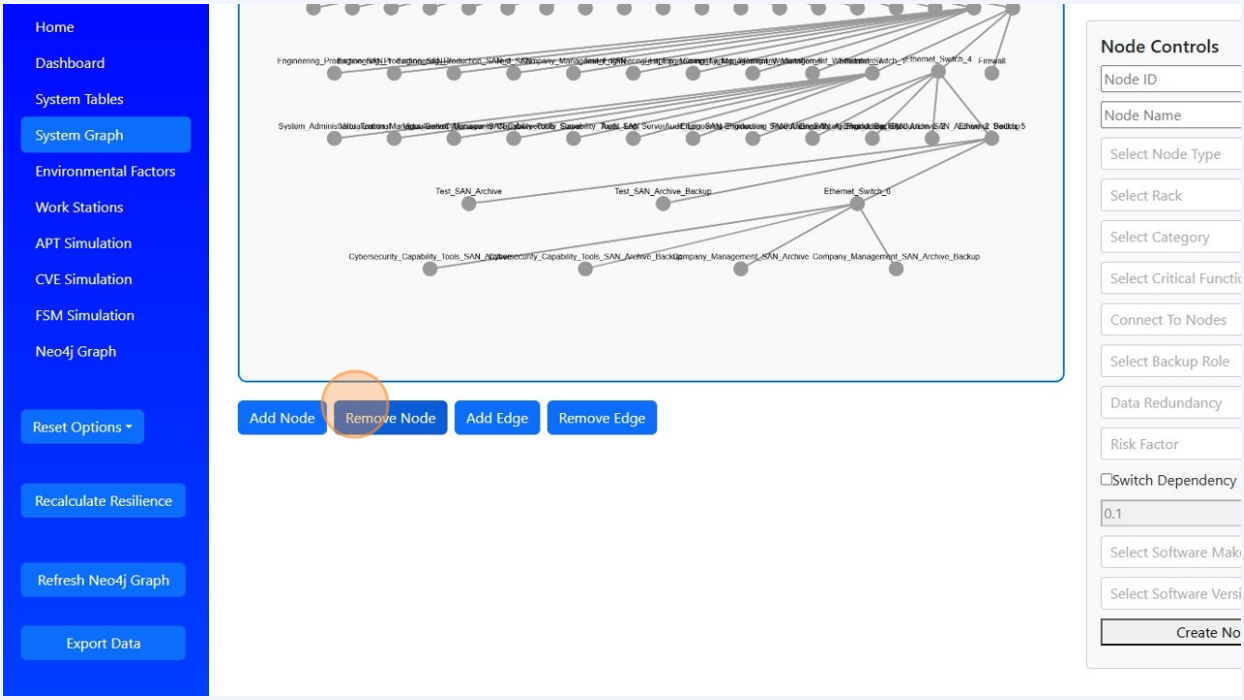
40 Input the prescribed information on the right



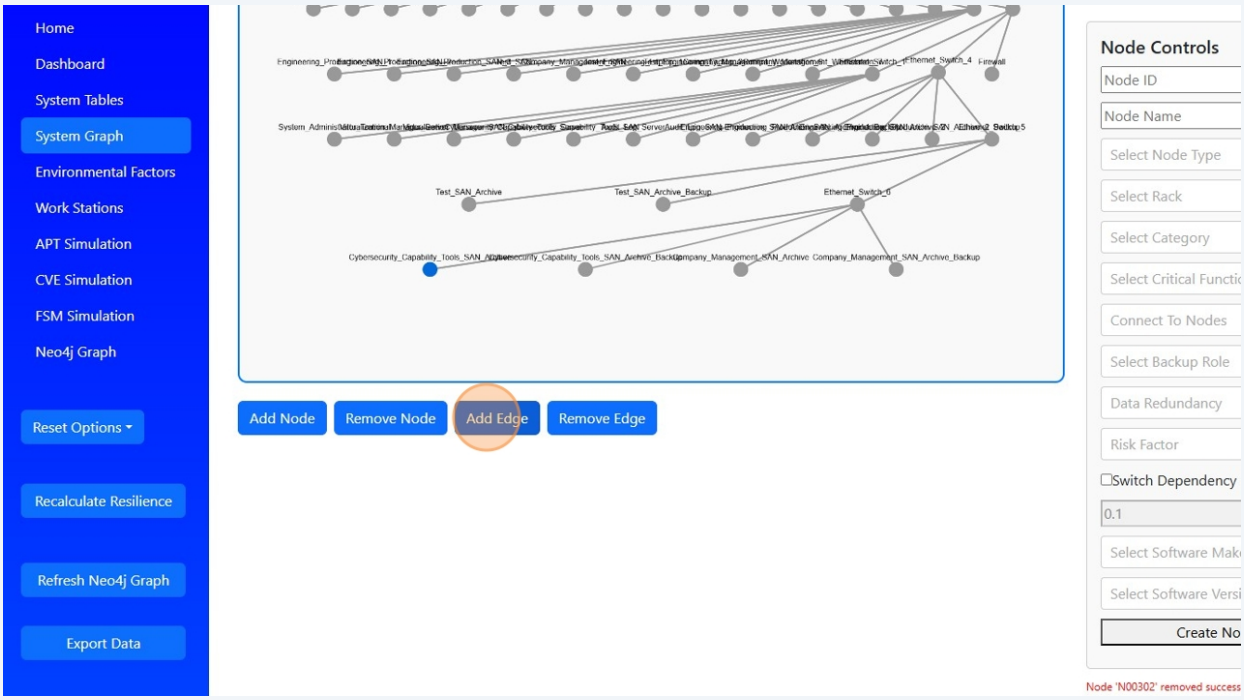
41 Click "Create Node" to add the node. Refresh the graph at the top to view the new node within the system.



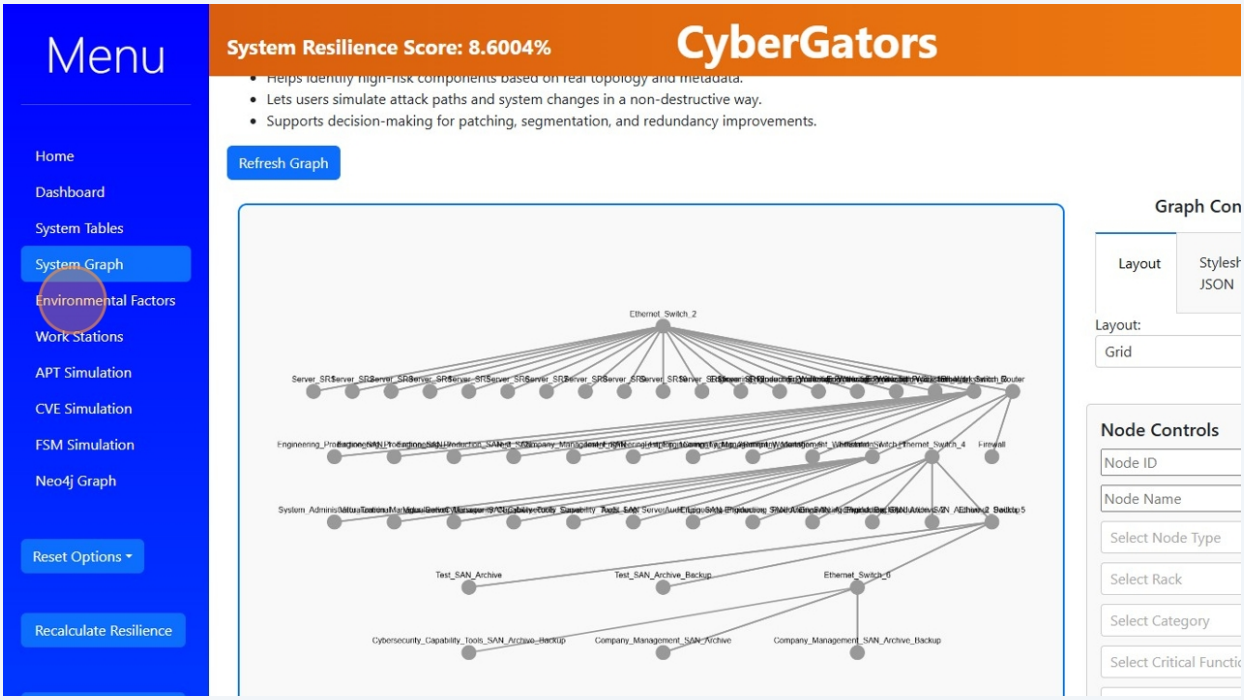
42 To remove a node, click a node on the graph, and then click "Remove Node", followed by refresh system graph.



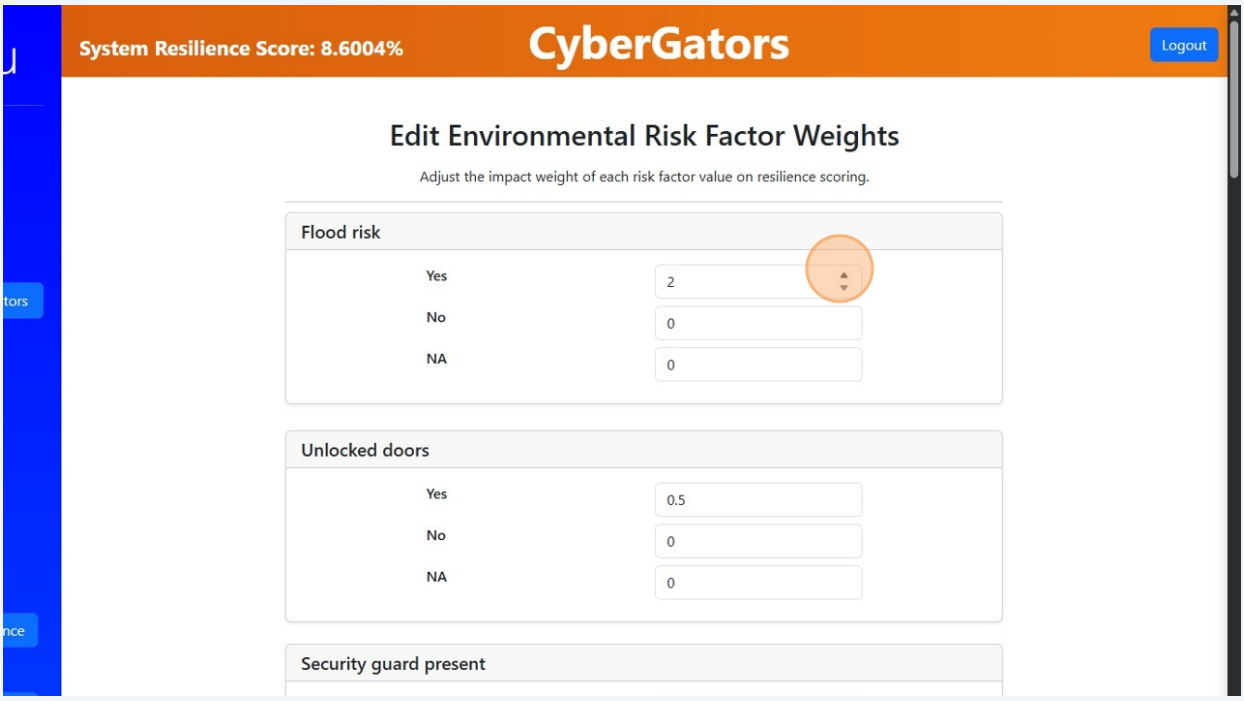
43 Select a node and then hit "Add Edge" to modify the edges of a given node



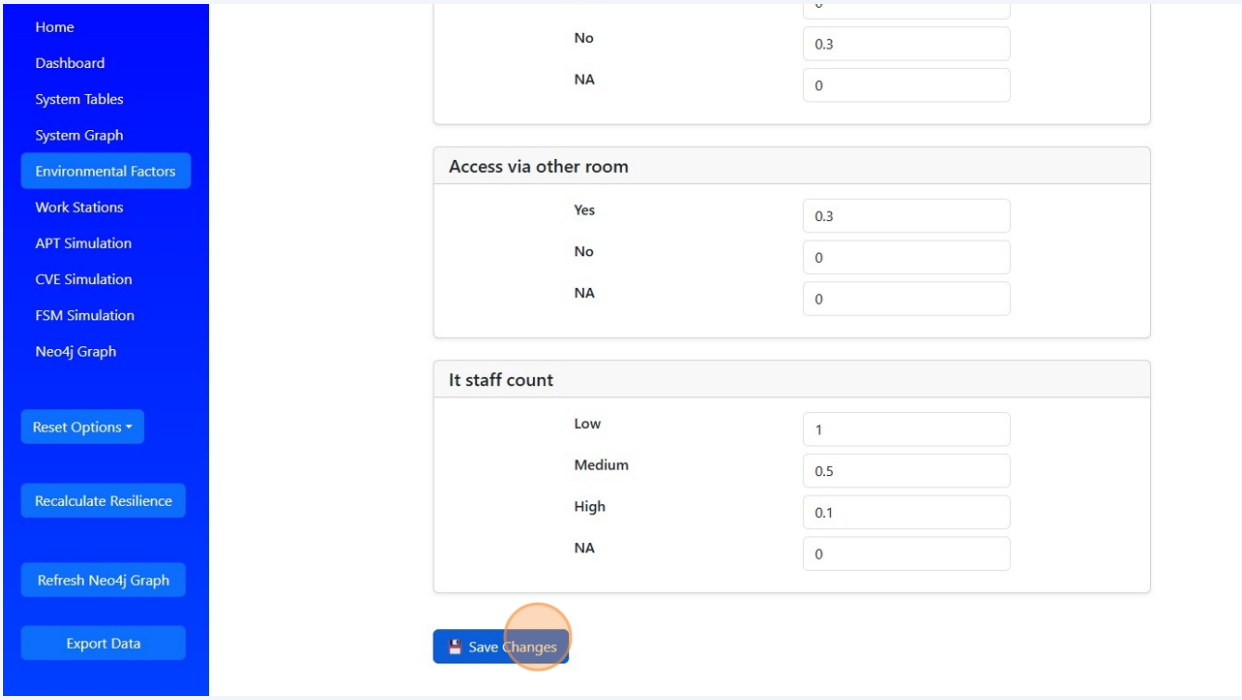
44 To view and edit the environmental risk factors, click "Environmental Factors"



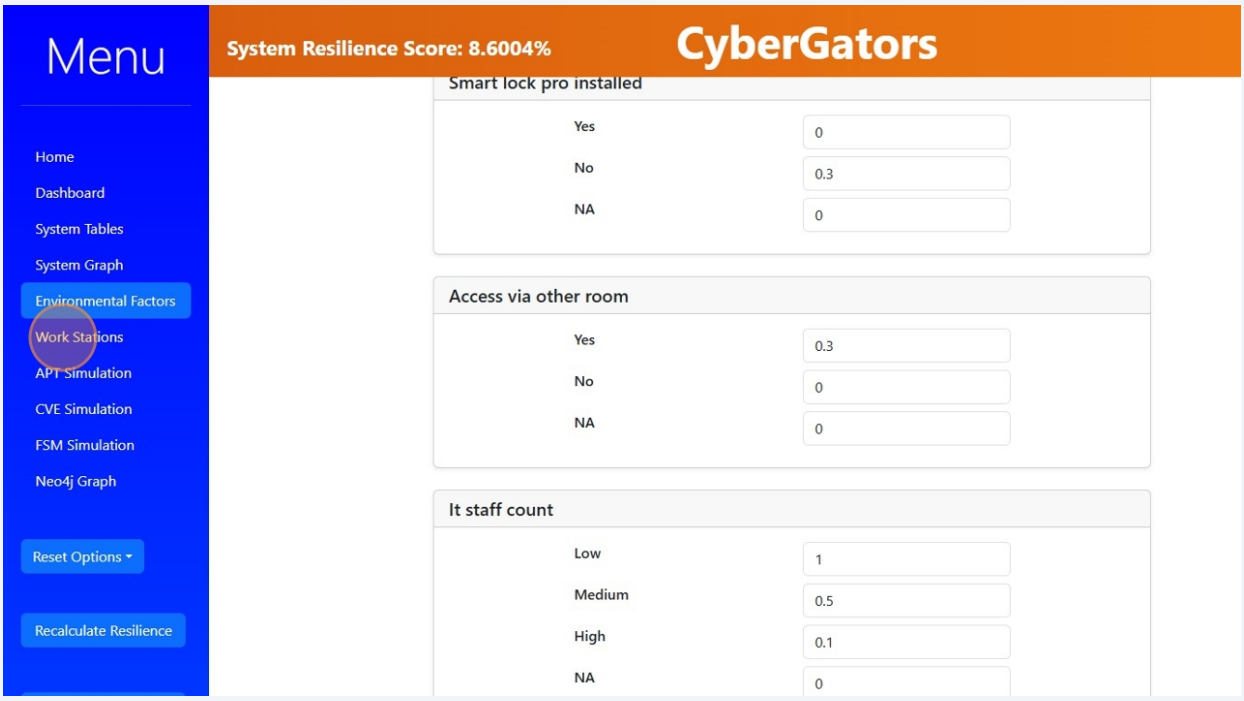
45 Edit the environmental risk factors by adjusting the number field to the right of each risk factor.



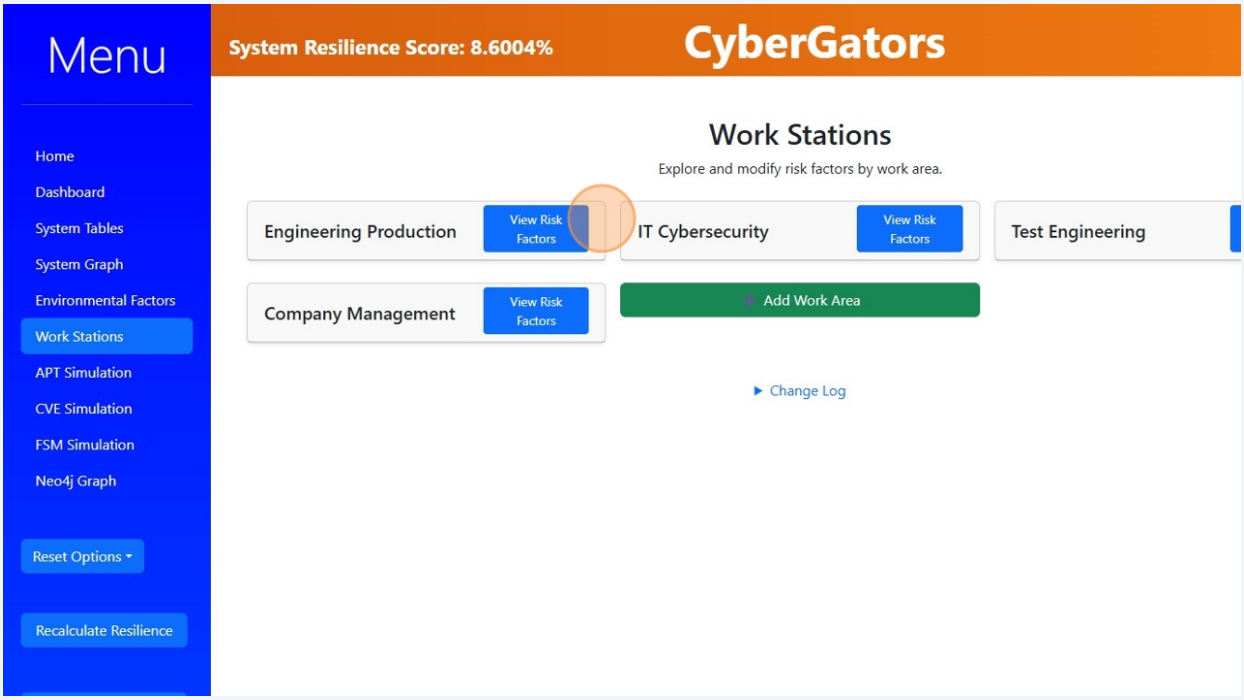
46 Click "💾 Save Changes" to save the changes to the environmental risk factors.



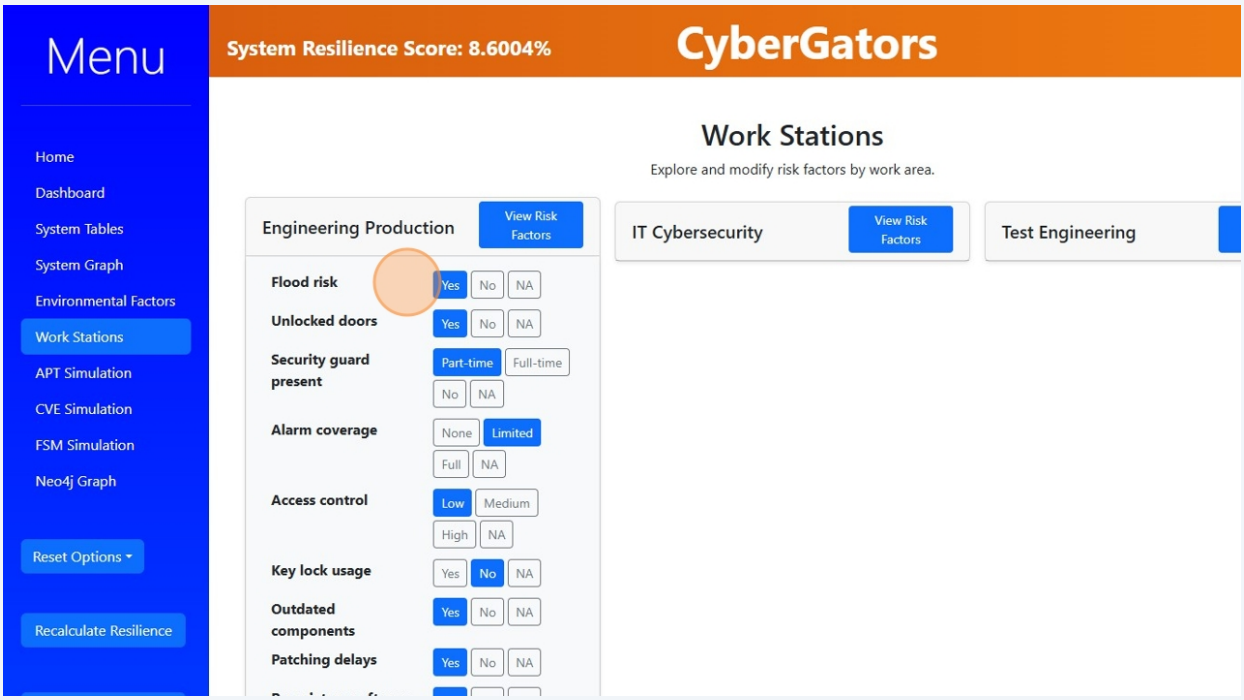
47 To view the work stations within the system, click "Work Stations"



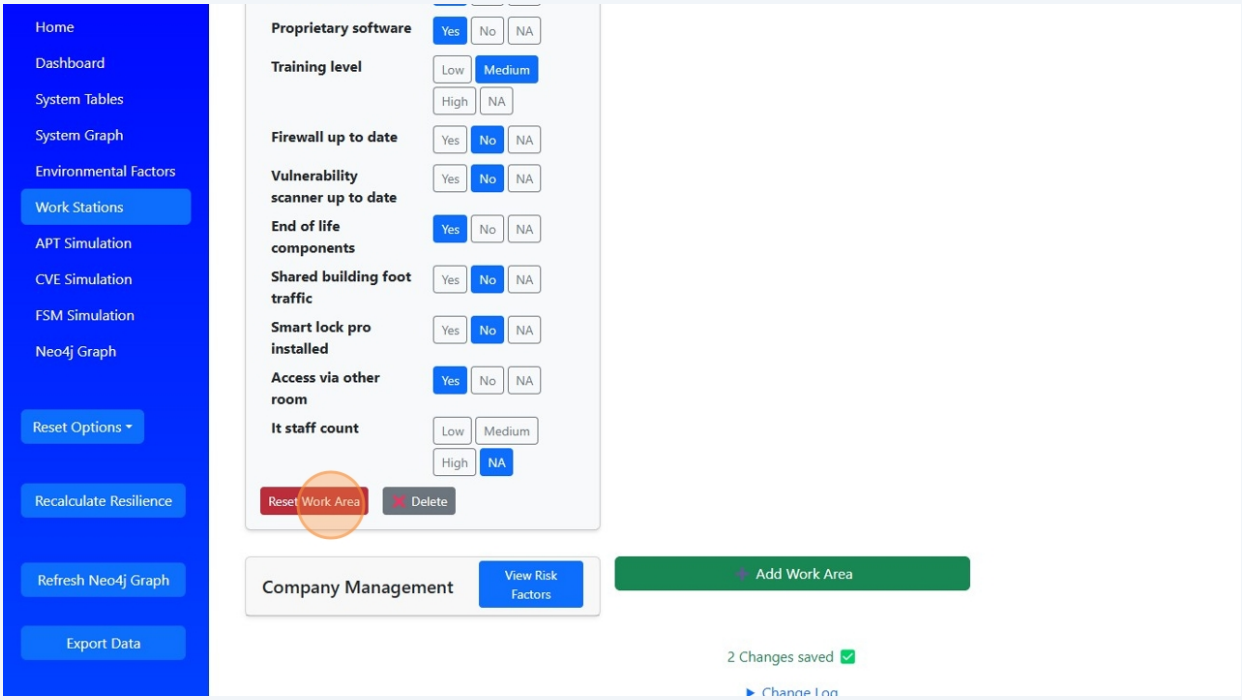
48 Work stations and their associated risks can be viewed by clicking the "View Risk Factors" button by each workstation.



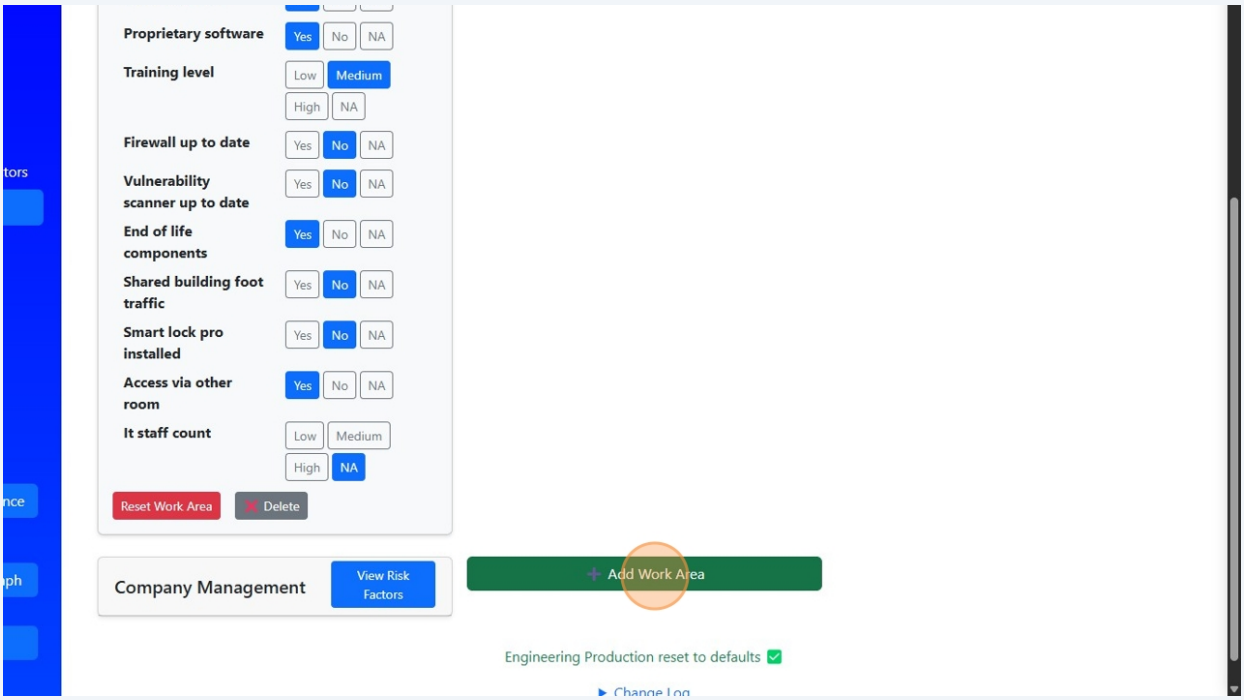
49 Make changes to the Risk Factors of a given workstation by using the scales built int Environmental Factors page.



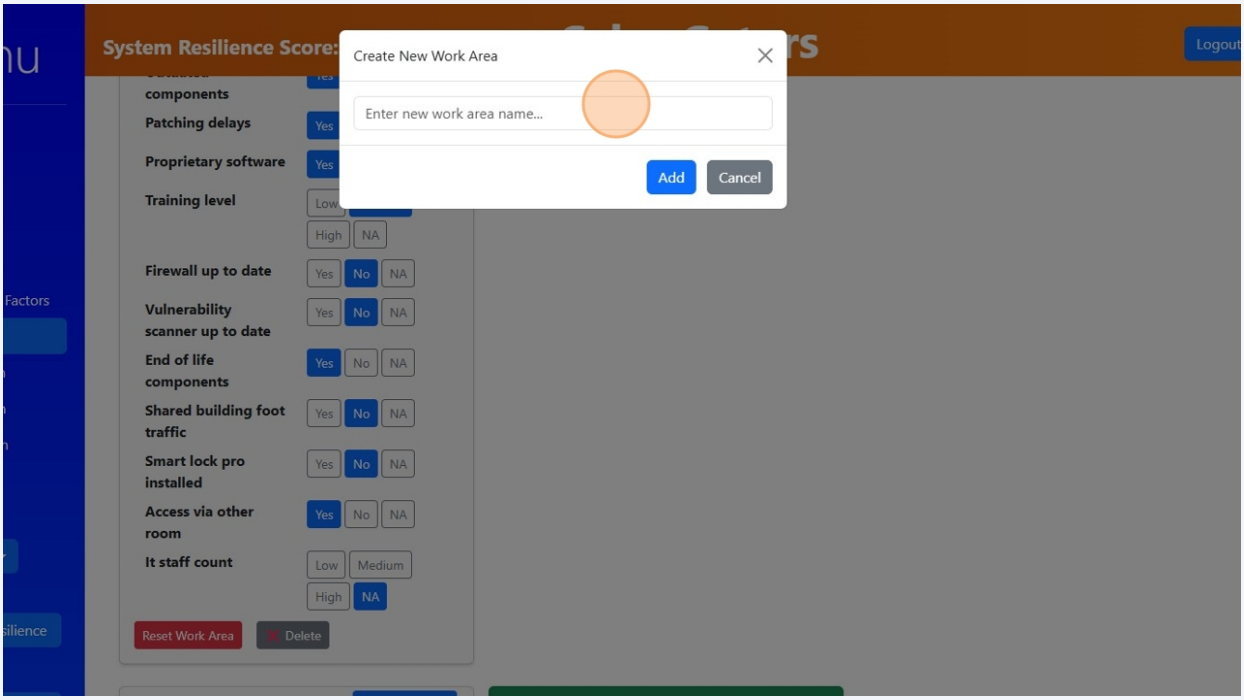
50 To reset the work area back to its initial values click "Reset Work Area". Or, select Delete to remove a work station.



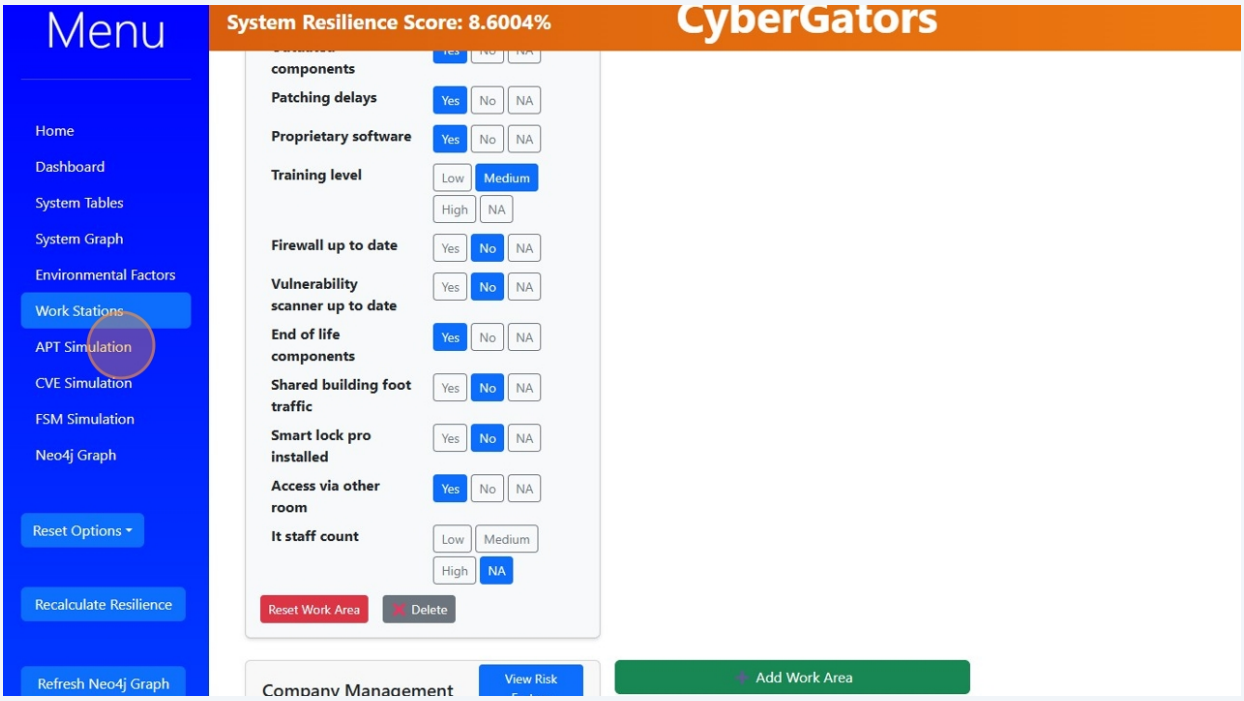
51 Click "⊞ Add Work Area" to add a work area to the system.



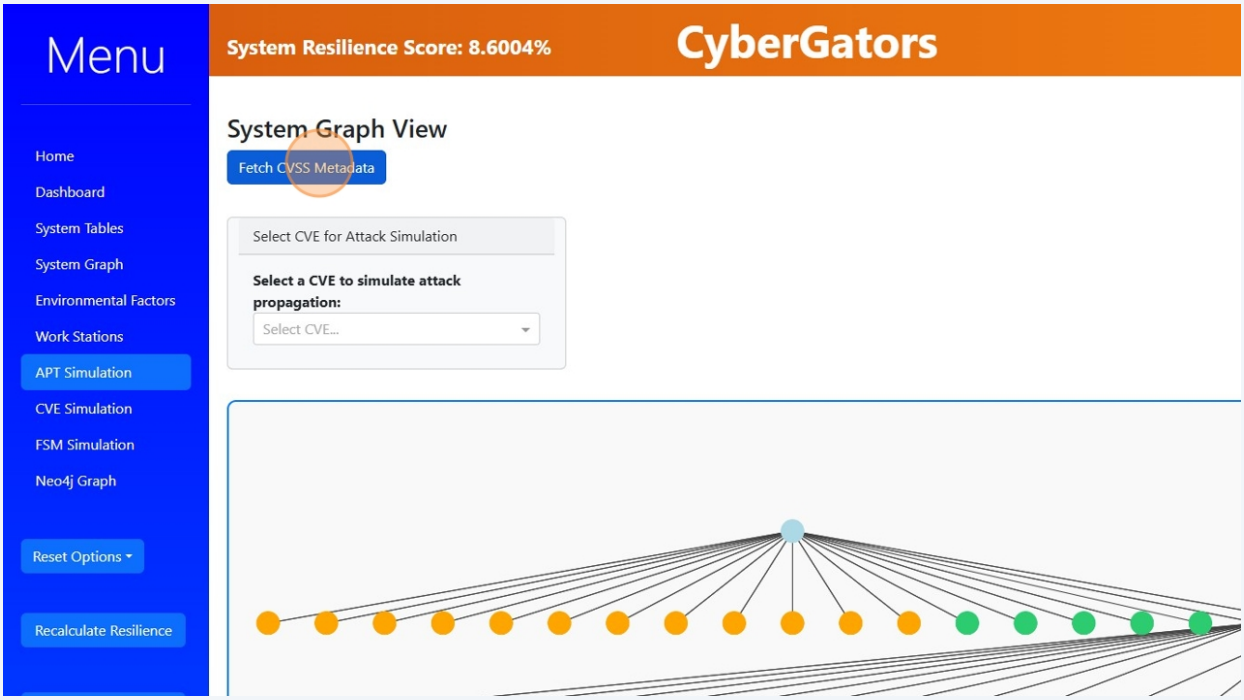
52 Give it a name and hit "Add." the new work area will be built with the same environmental risk factors as the other stations.



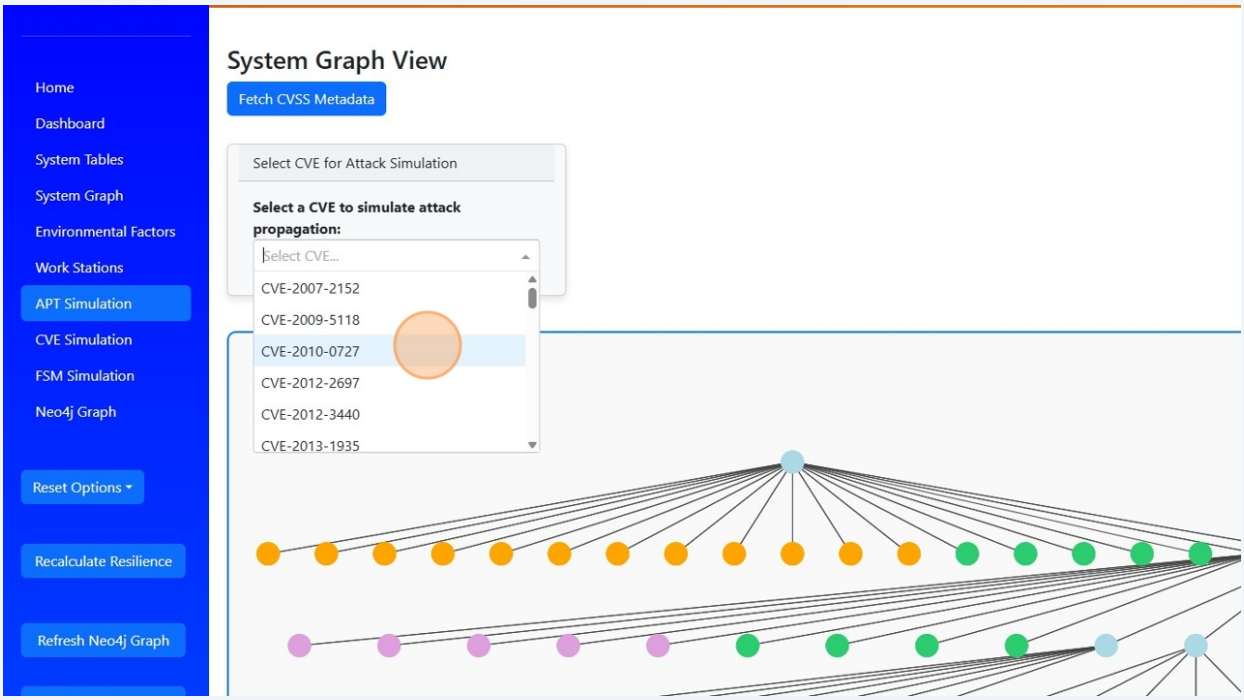
53 To view the Advanced Persistent Threat Simulation, Click "APT Simulation"



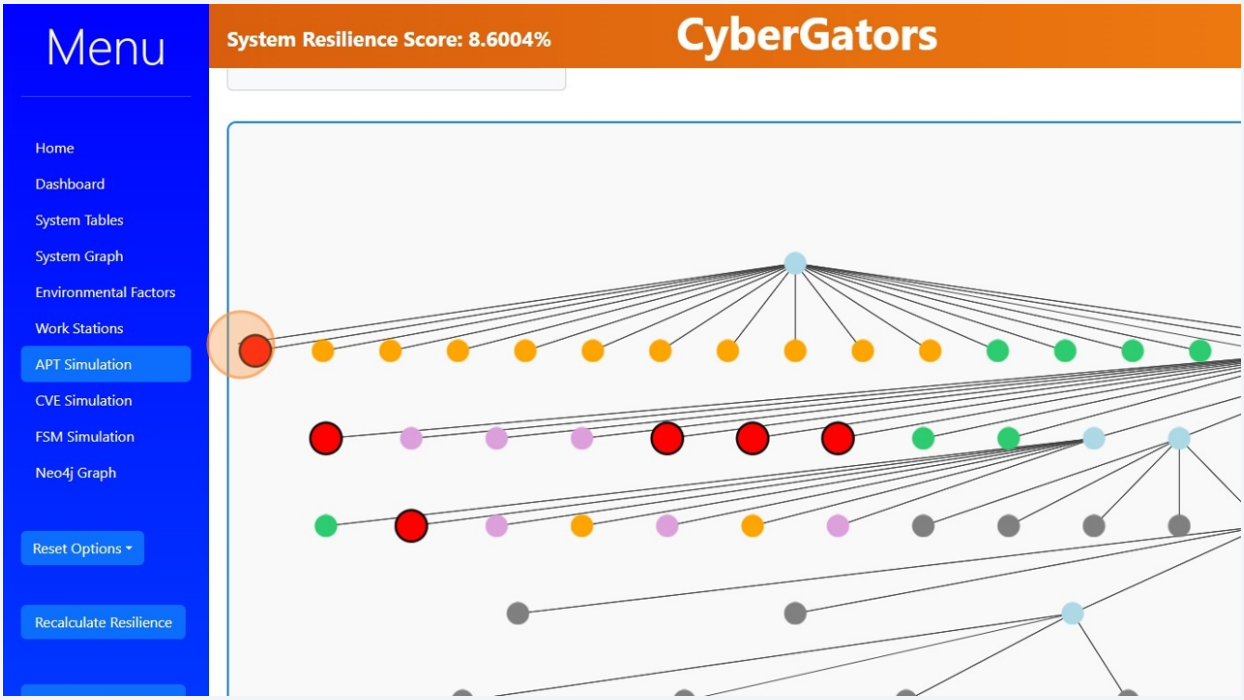
54 Click "Fetch CVSS Metadata" to fetch most up to date CVSS metadata from MITRE.



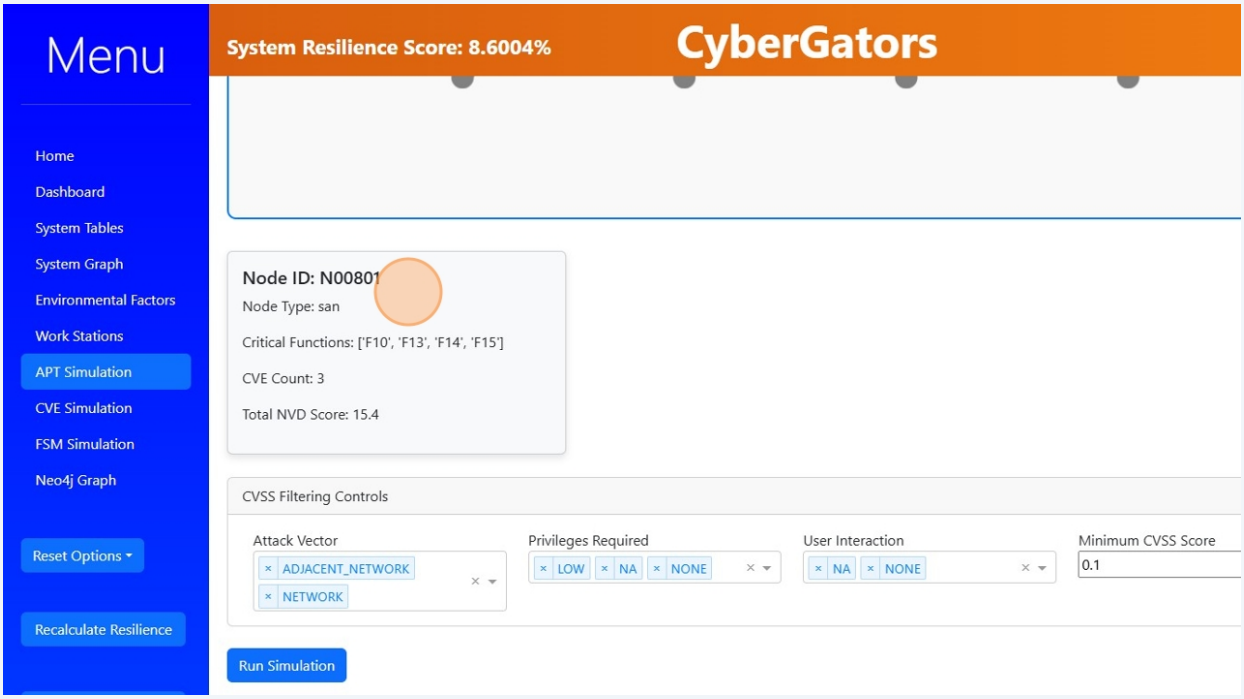
55 Click "Select CVE..." to select which CVE to exploit within the system.



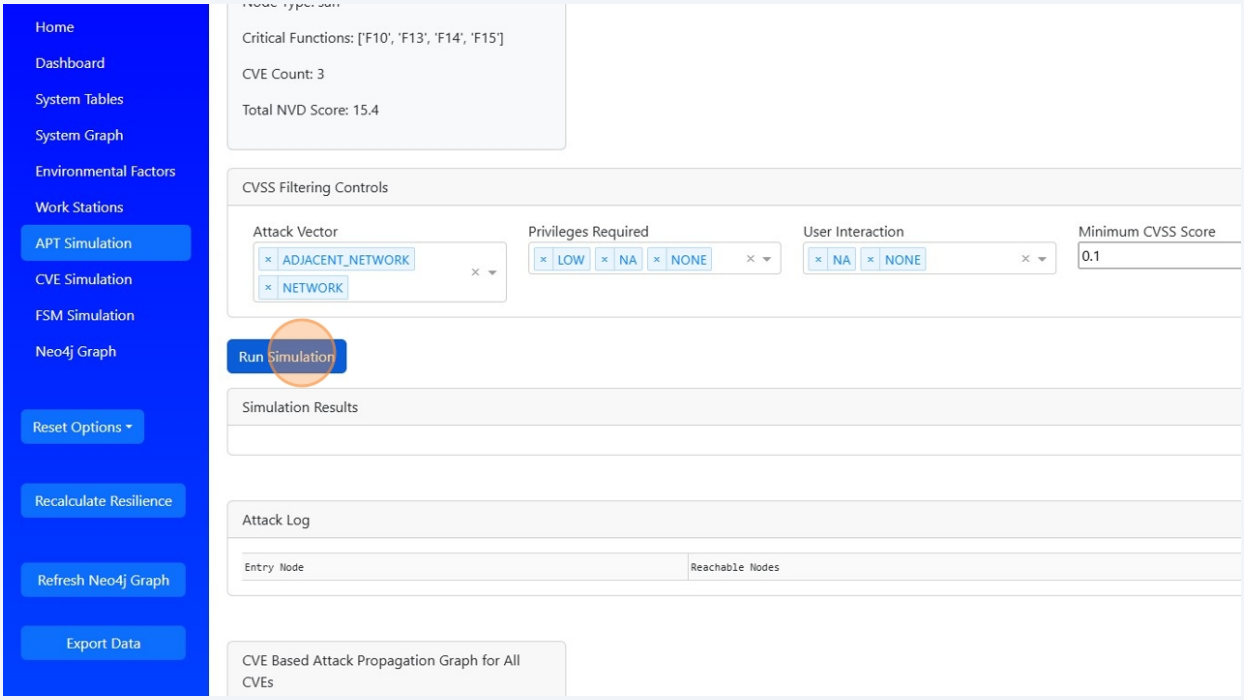
56 View the nodes that contain that exploited CVE within the system on the first graph



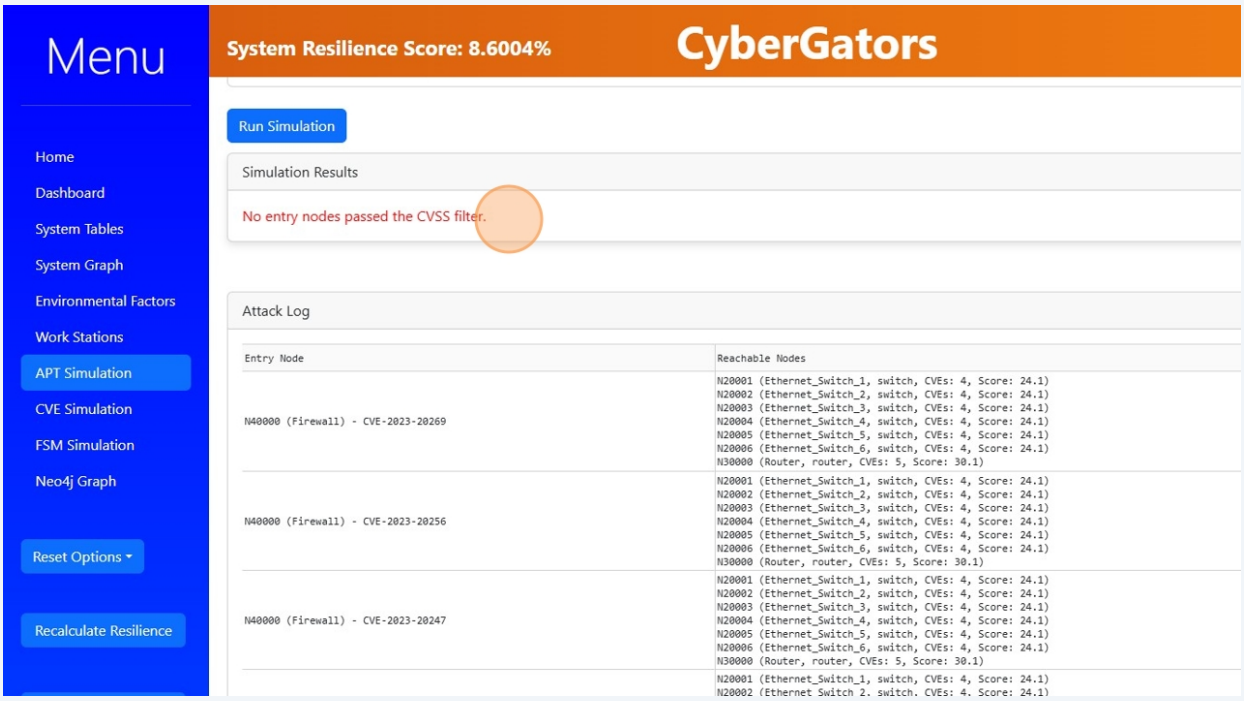
57 Selecting a highlighted node will reveal more information about the node that is under attack, as well as information about the associated attack vector, required privileges, if user interaction is necessary for exploitation, and minimum CVSS score.



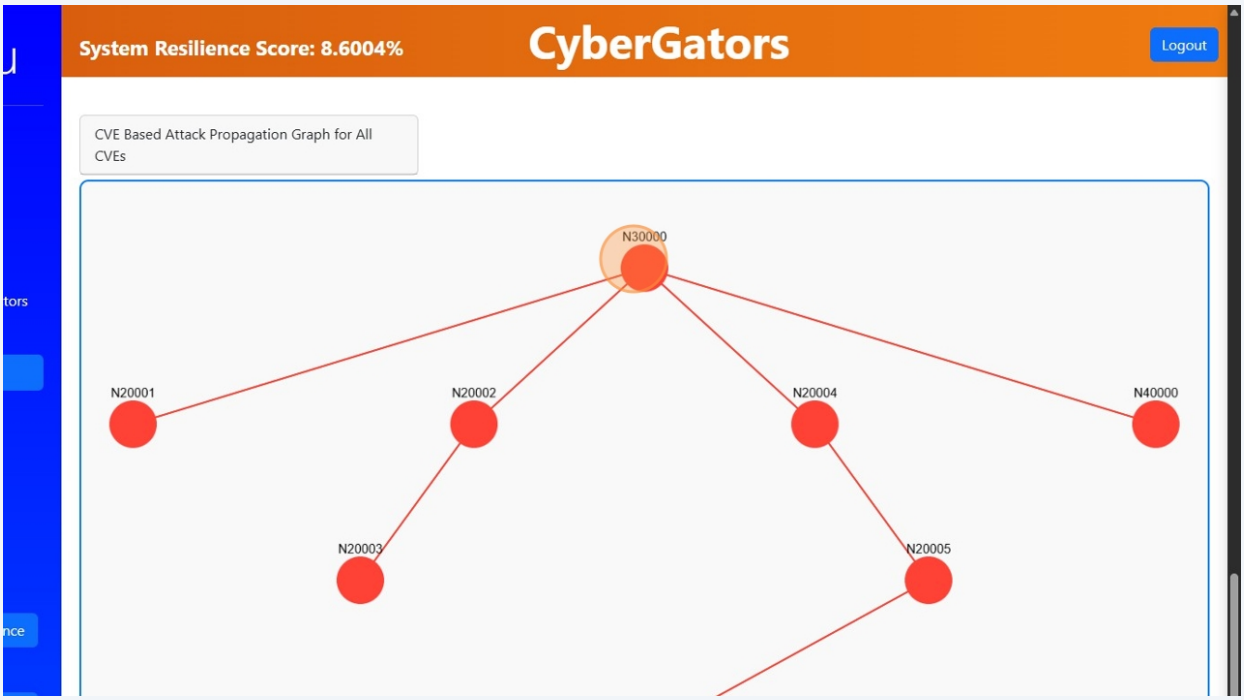
58 To run the exploitation simulation on the selected node, click "Run Simulation"



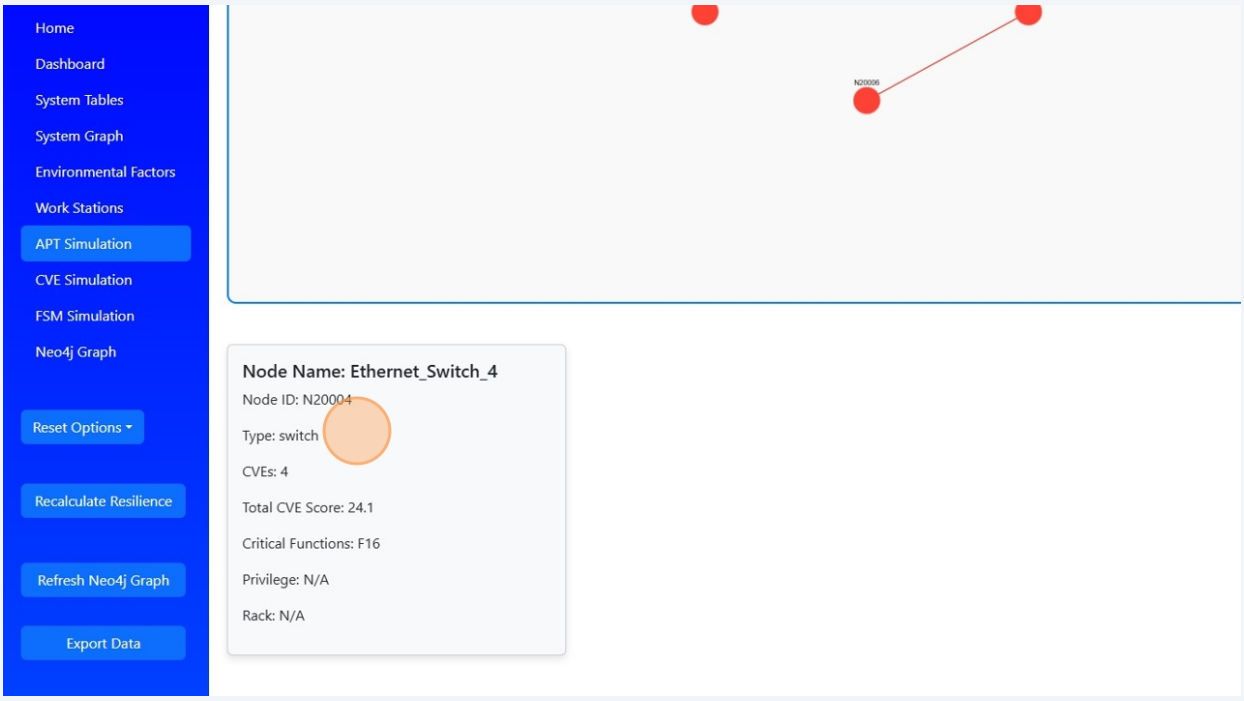
59 The simulation results will populate below, along with a comprehensive attack log and the nodes/CVEs attacked and exploited



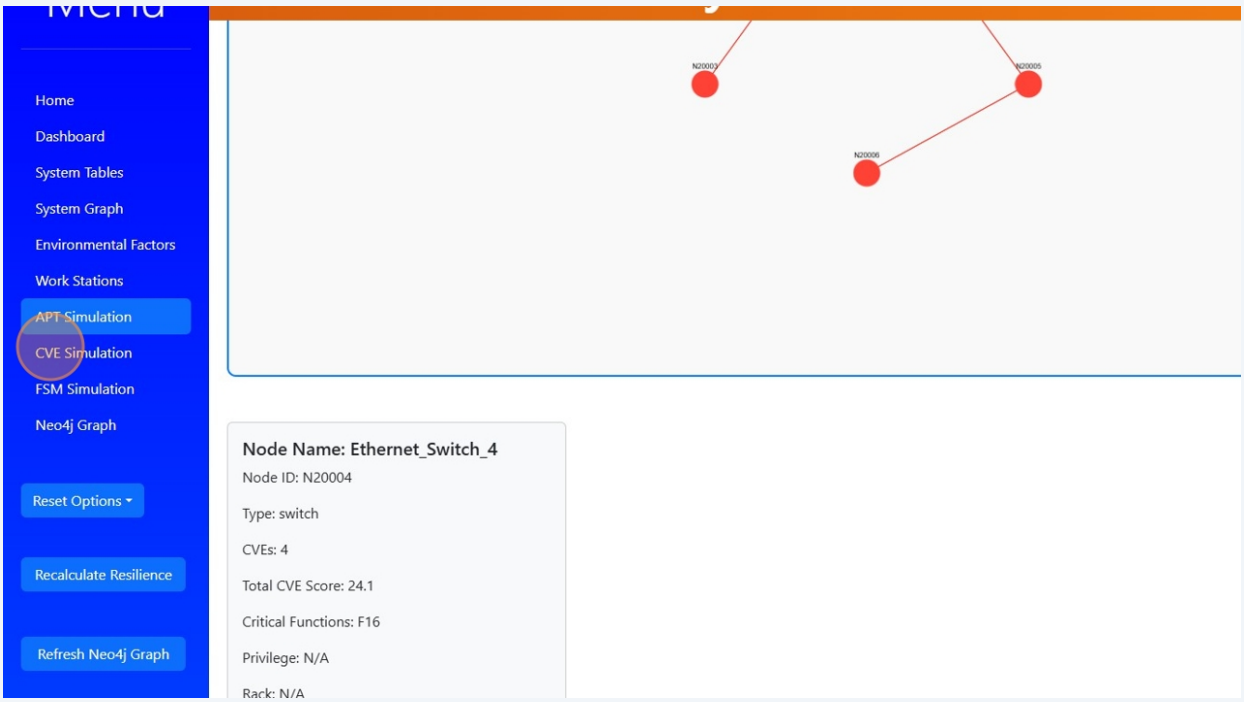
60 Scroll down further to see the CVE Based Attack Propagation Graph for All CVEs. This shows the traversal through the system based on the node IDs and the exploited CVE and attack log.



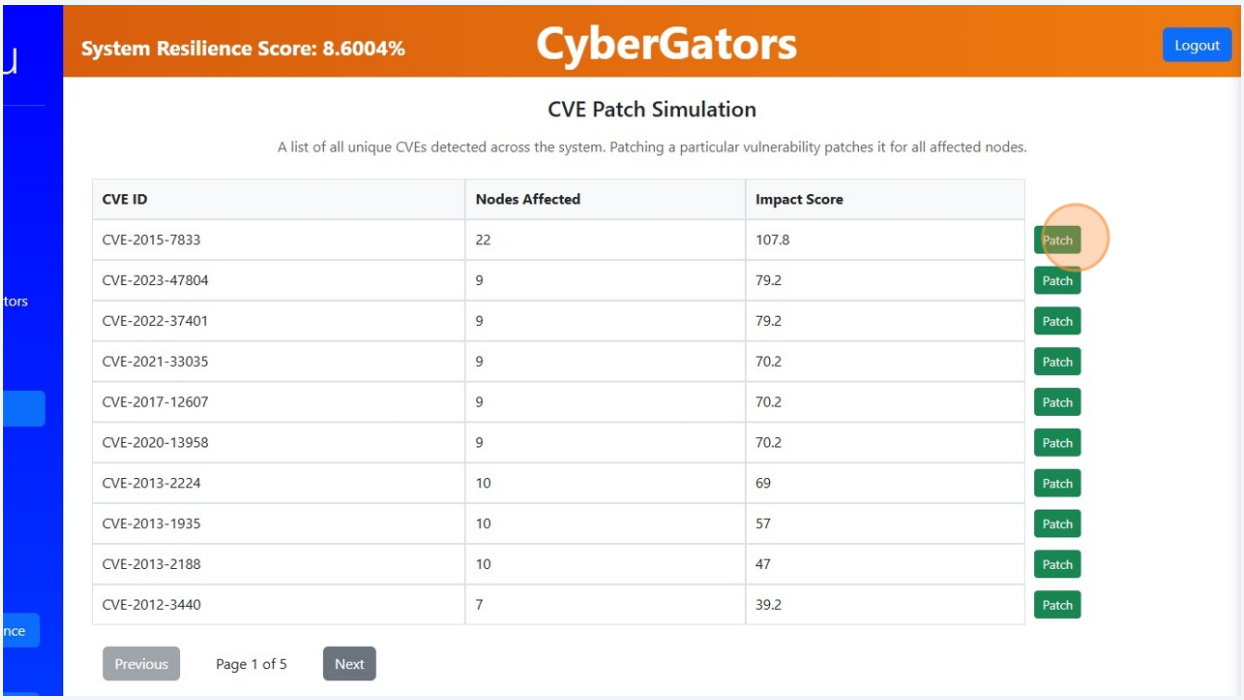
61 At the very bottom, when a node is selected, more information about the node populates, including the node type, ID, total CVEs, total CVE score, any critical functions, if it exists on a server rack, or requires a certain privilege level to access.



62 Next, to view the CVE Patch Simulation, click "CVE Simulation"

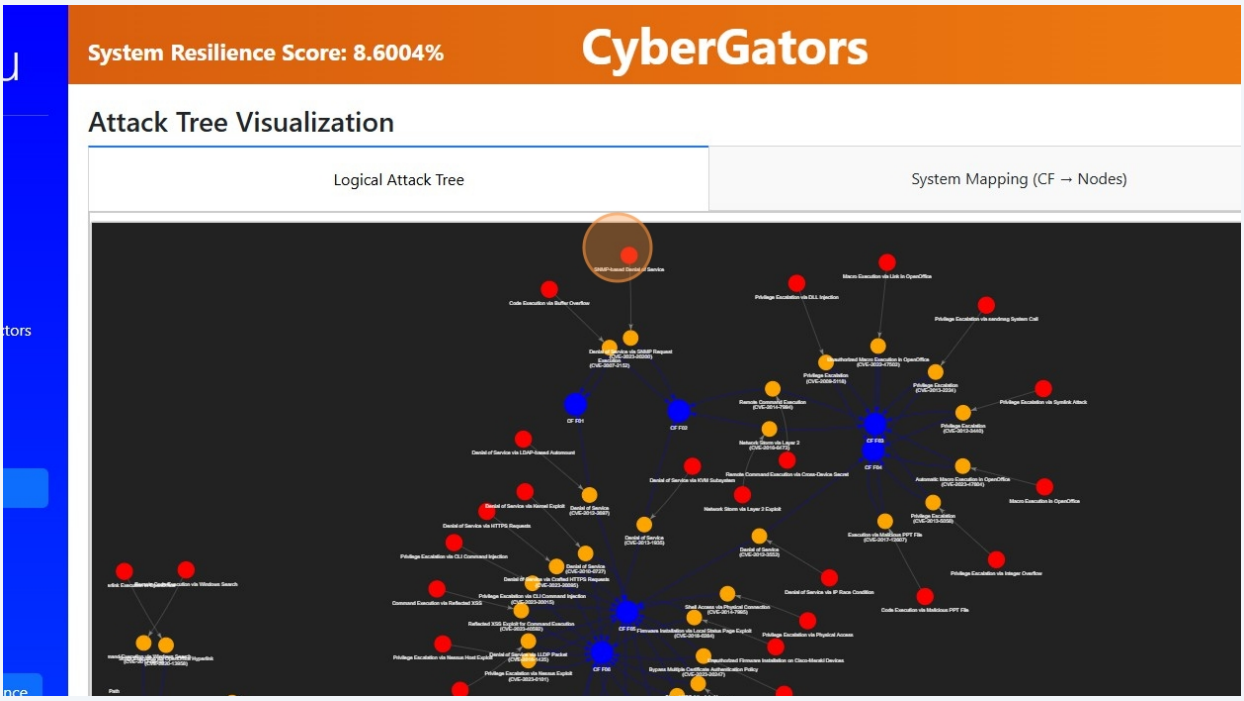


63 To simulate patching a CVE within the system, click "Patch" next to the CVE you wish to patch.

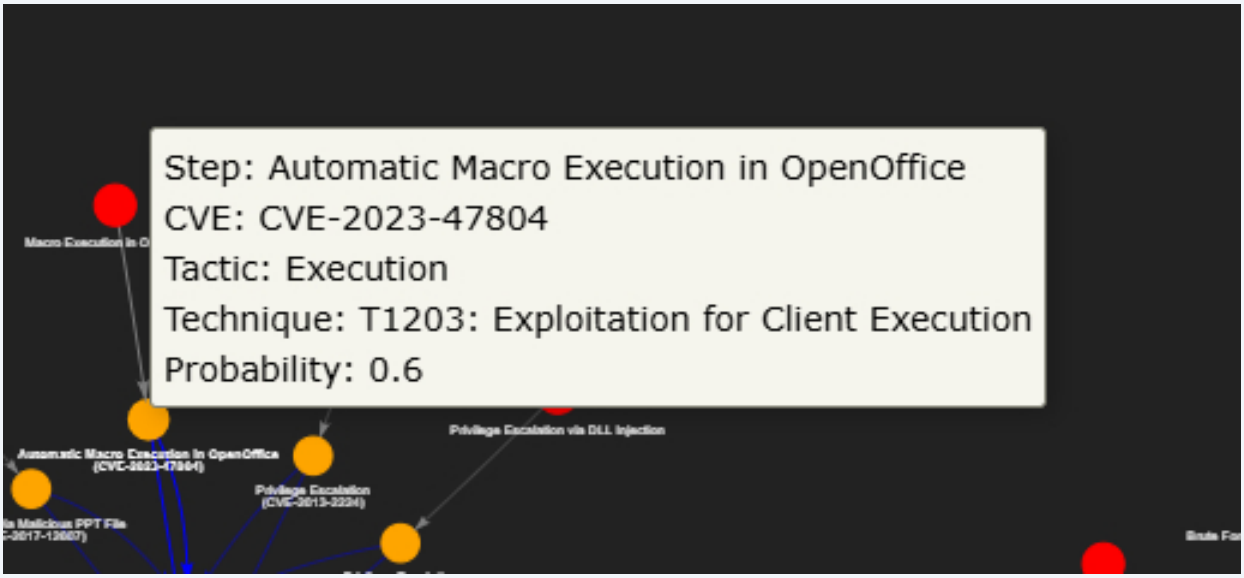


64 Next, to view the Free State Machine Simulation and Attack Tree Visualization, click "FSM Simulation"

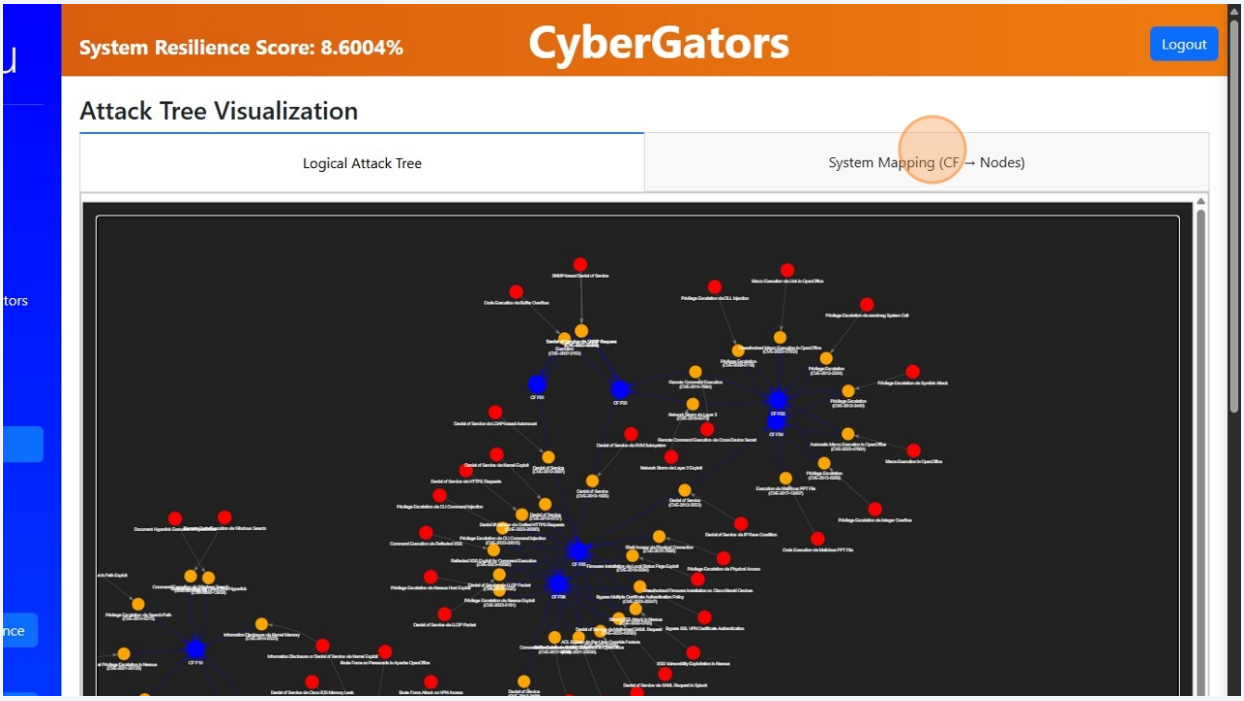
65 Select a starting node on the edge of the graph to begin traversing the Attack Tree (see Logical Attack Tree)



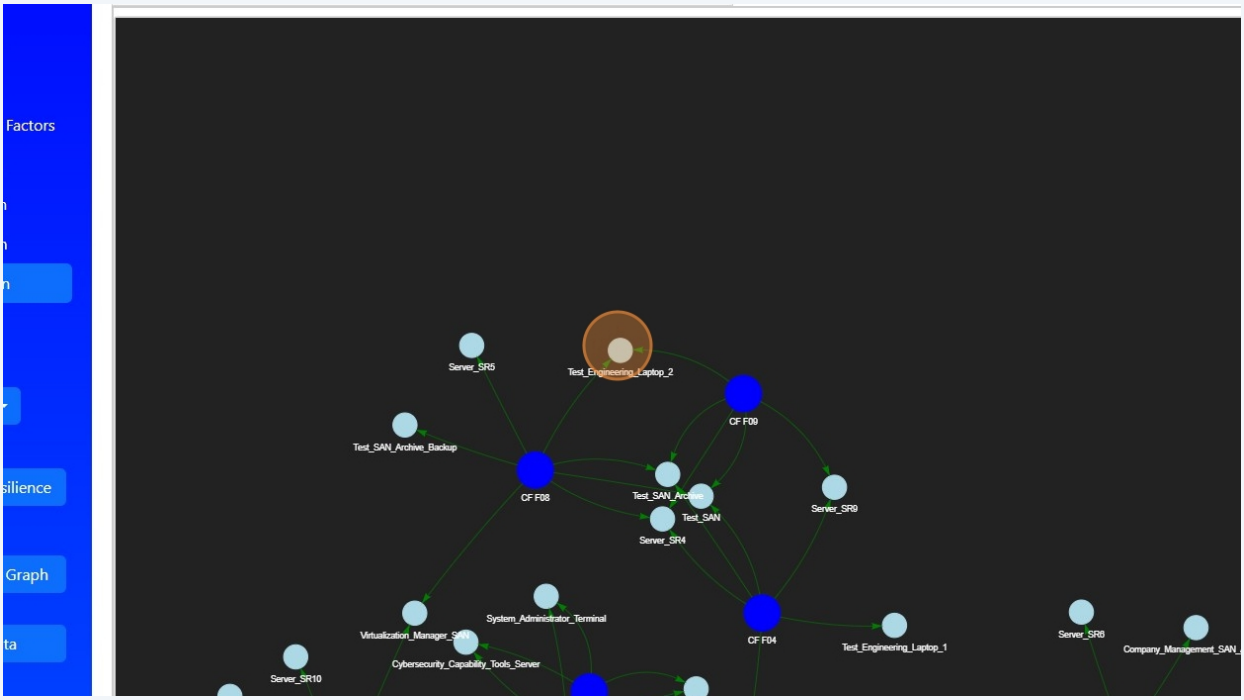
66 Selecting the next node reveals the traversal information, including the penetration tactic, tactic, exploited CVE, and probability of success



67 To view the association between the nodes and Critical Functions, click "System Mapping (CF → Nodes)"



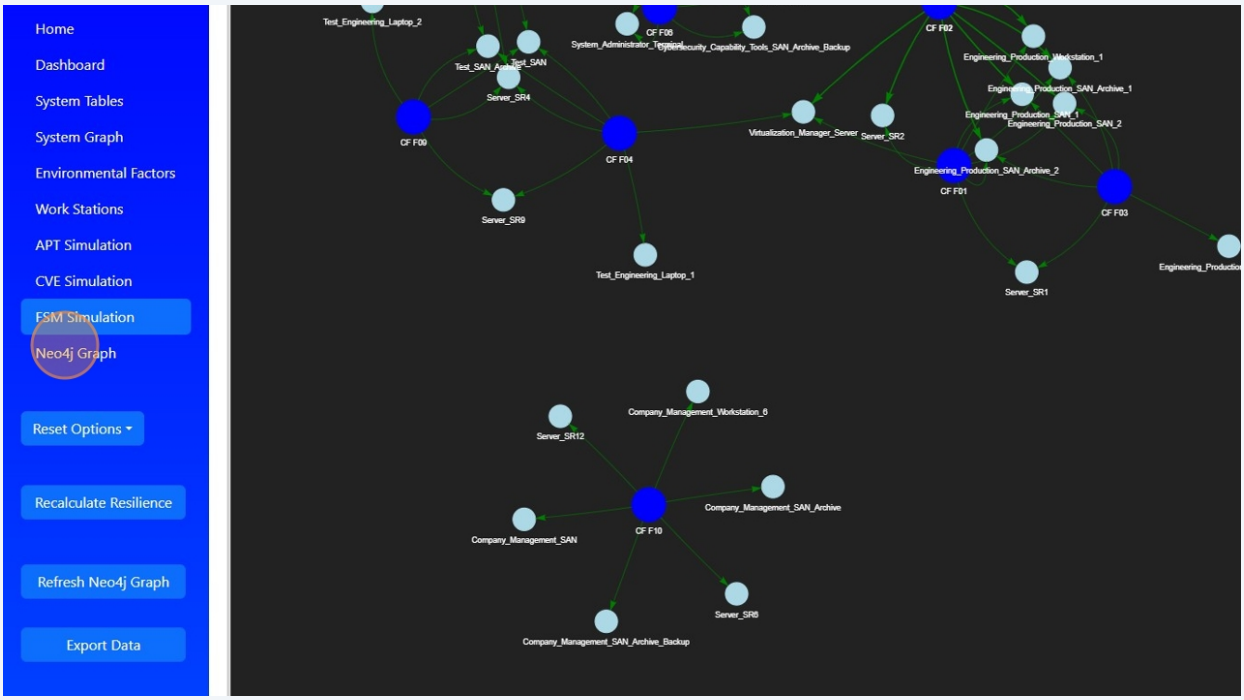
68 To start the simulation, select the starting node.



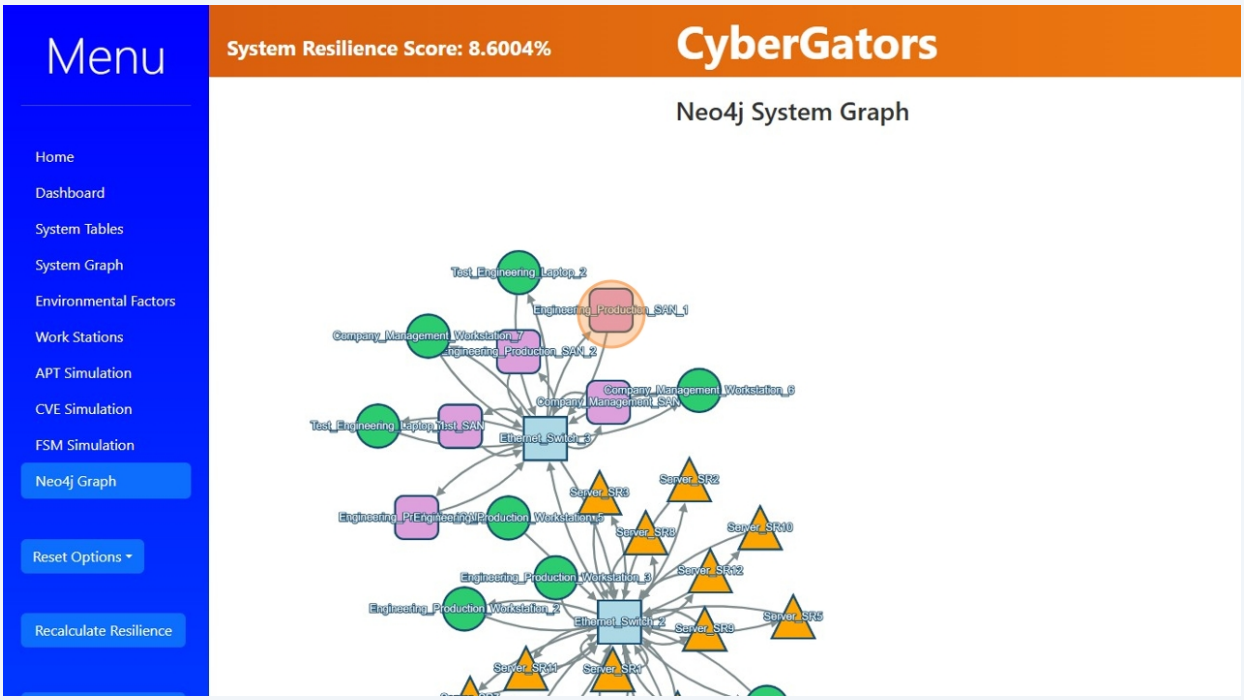
69 Select the traversal node

70 This reveals more information about the traversal nodes and total CVE score on a given node, as well as directed edges along with the attack could traverse.

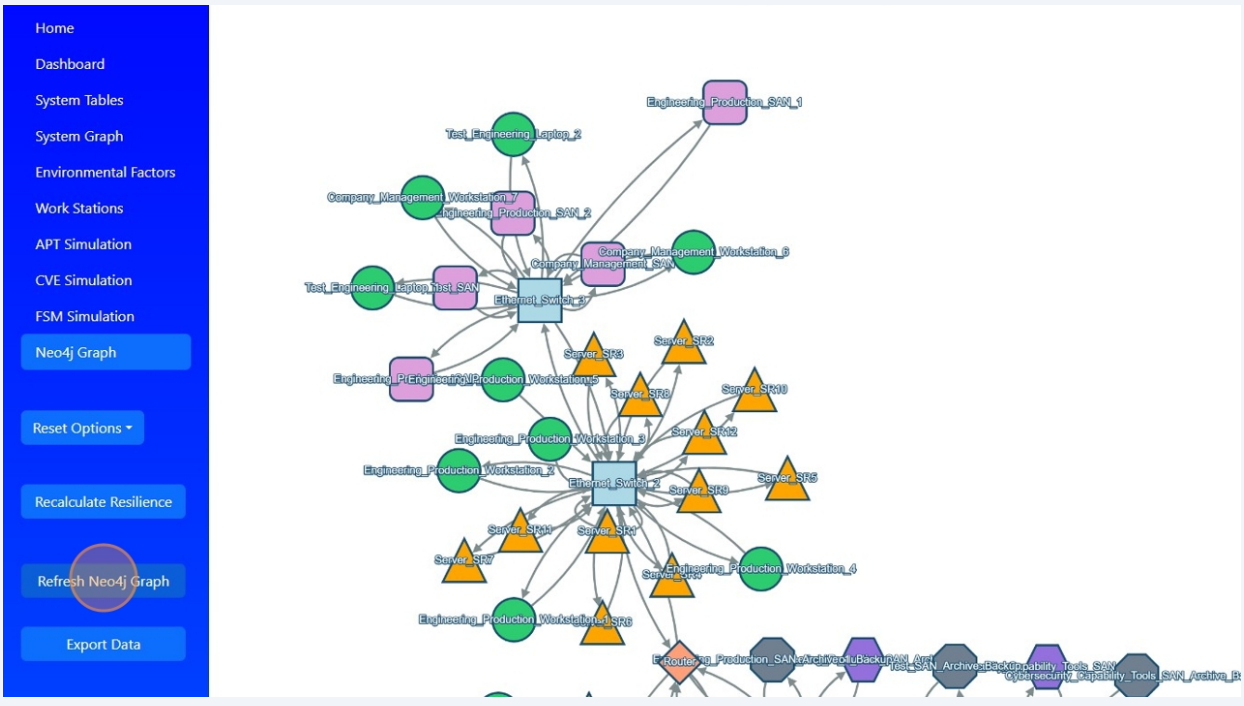
71 To view the Neo4j graph which is linked to the database containing the system, click "Neo4j Graph"



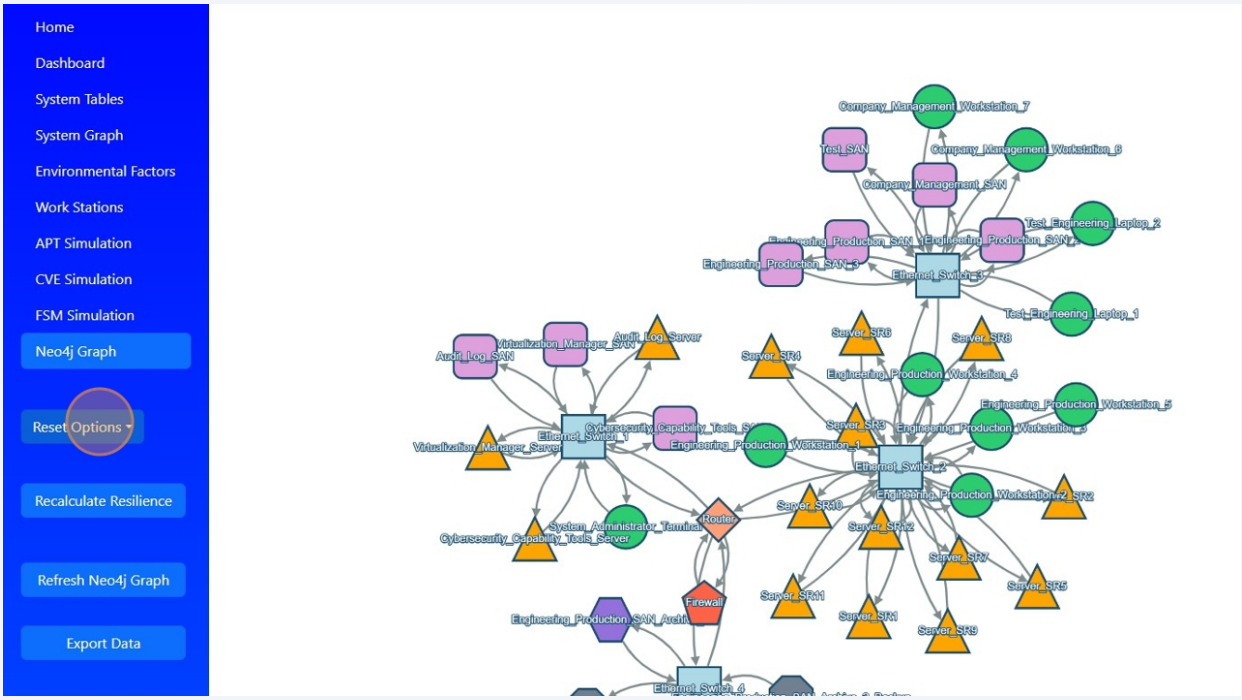
72 The Neo4j graph is the start of a combination of the previous tables using a database versus raw JSON files. It remains a work in progress but actively shows the nodes within the system and their associations through directed edges.



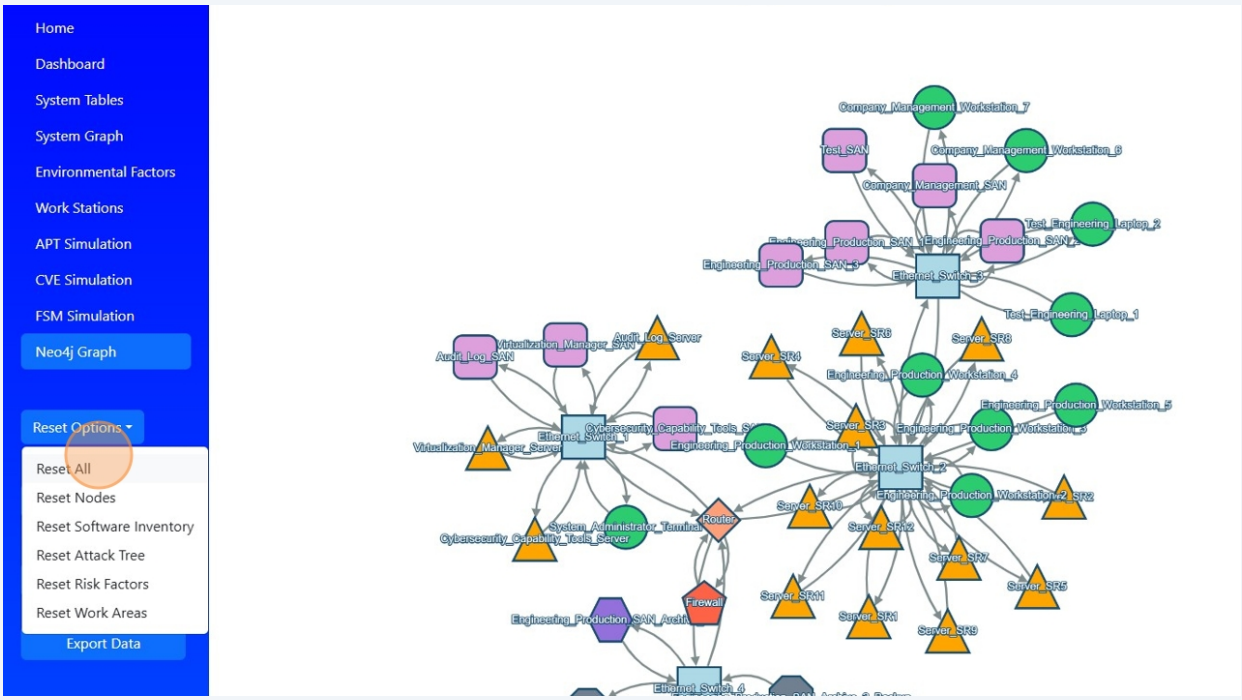
73 To refresh the graph, click "Refresh Neo4j Graph"



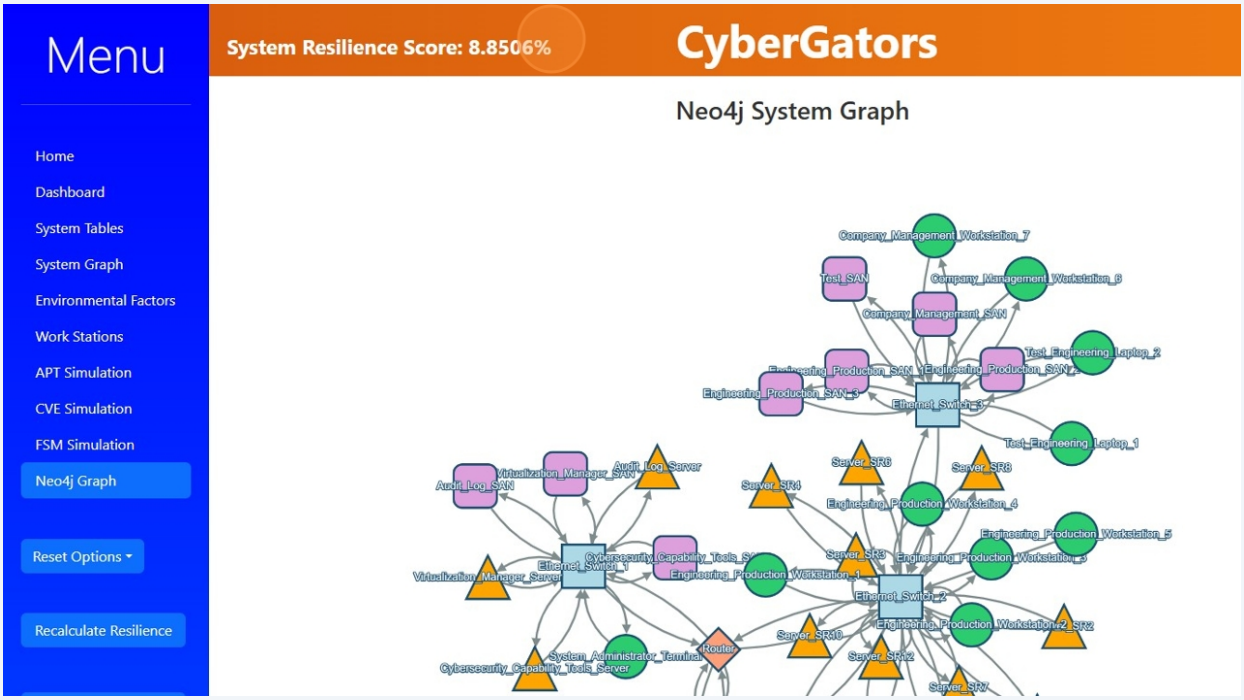
74 To reset any of the changes made back to the original system settings, click "Reset Options"



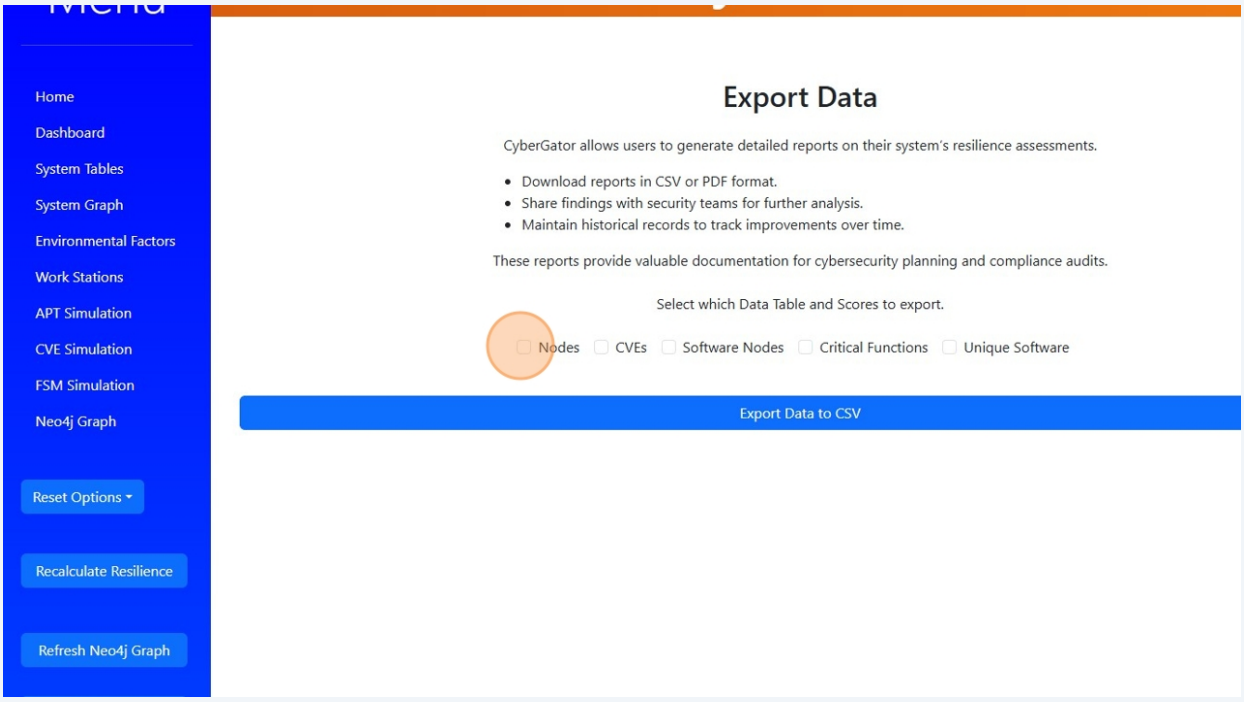
75 To reset any of the changes made back to the original system settings, click "Reset Options" and select which components to reset.



76 To recalculate the resilience of the system, click "Recalculate Resilience" on the sidebar, and notice that the System Resilience Score updates on the top bar.



77 To export data, select the "Export Data" button the sidebar, select the data tables to export, and then Export to CSV button. To capture the System Resilience Score, navigate back to the Dashboard and export the pie chart as described earlier.



78 To log out, simply click "Logout" in the upper righthand corner.