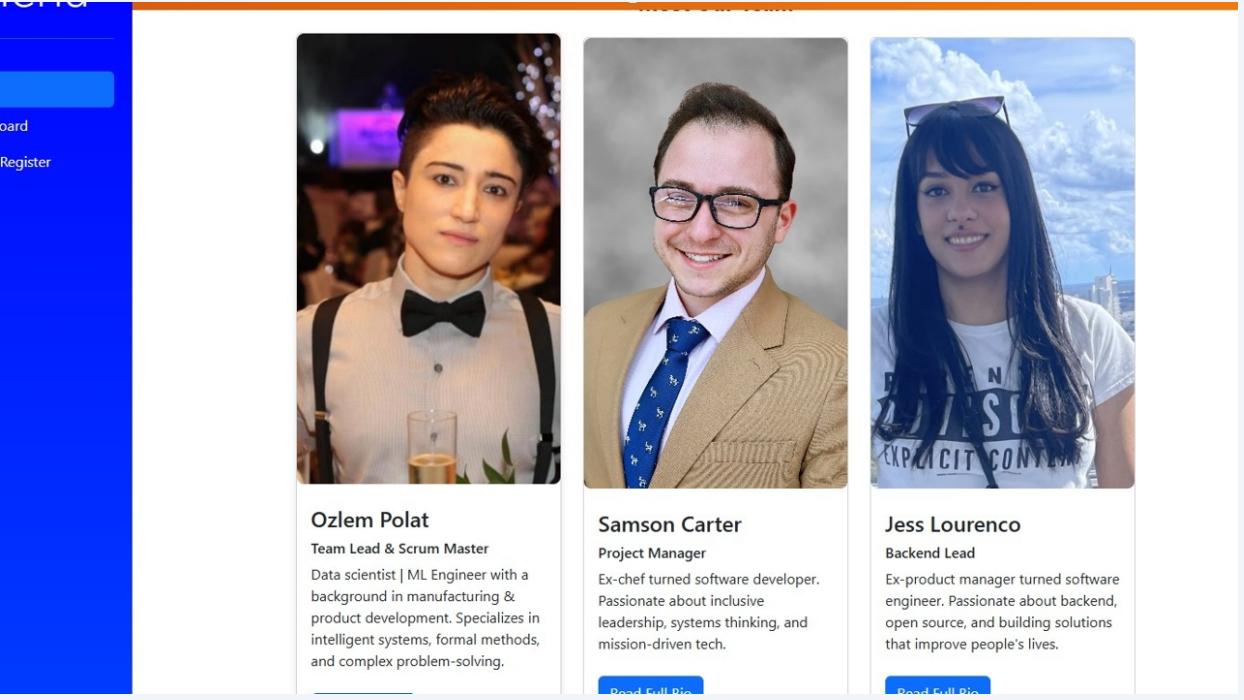


Navigating and Managing System Tables and Graphs

Scribe 

1

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



The screenshot shows a web application interface with a sidebar on the left containing 'Dashboard' and 'Register' buttons. The main content area displays three team member profiles in cards:

- Ozlem Polat**
Team Lead & Scrum Master
Data scientist | ML Engineer with a background in manufacturing & product development. Specializes in intelligent systems, formal methods, and complex problem-solving.
[Read Full Bio](#)
- Samson Carter**
Project Manager
Ex-chef turned software developer. Passionate about inclusive leadership, systems thinking, and mission-driven tech.
[Read Full Bio](#)
- Jess Lourenco**
Backend Lead
Ex-product manager turned software engineer. Passionate about backend, open source, and building solutions that improve people's lives.
[Read Full Bio](#)

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.

The image shows a mobile application's home screen. On the left is a sidebar with 'Home', 'Dashboard', and 'Login/Register'. The main area displays three team member profiles in cards:

- Ozlem Polat**
Team Lead & Scrum Master
Data scientist | ML Engineer with a background in manufacturing & product development. Specializes in intelligent systems, formal methods, and complex problem-solving.
[Read Full Bio](#) (button is circled in yellow)
- Samson Carter**
Project Manager
Ex-chef turned software developer. Passionate about inclusive leadership, systems thinking, and mission-driven tech.
[Read Full Bio](#)
- Jess Lourency**
Backend Lead
Ex-product manager turned software engineer. Passionate about backend, open source, and building solutions that improve people's lives.
[Read Full Bio](#)

3

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

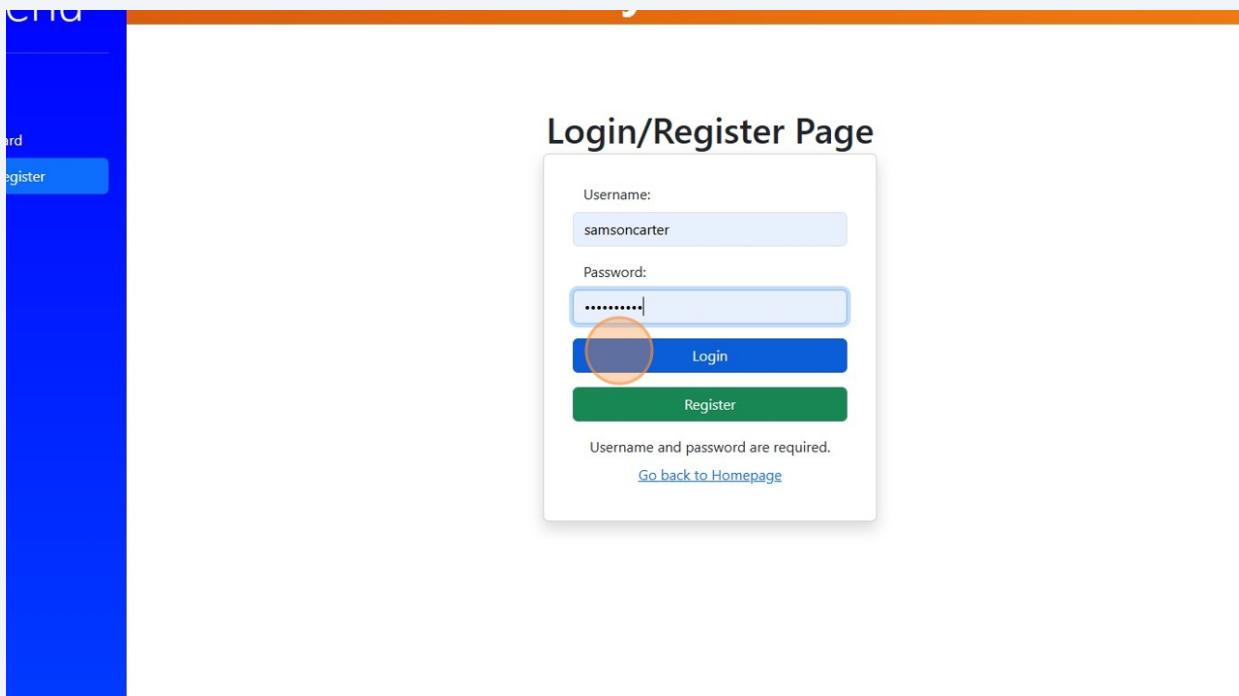
The image shows the CyberGators application interface. On the left is a sidebar with 'Home', 'Dashboard', and 'Login/Register' (button is circled in red). The main area has a header 'CyberGators' with a sub-header: 'Inference, & fuzzy logic-based risk scoring, CyberGator simulates how threats propagate across complex environments.' Below are three feature cards:

- Risk Assessment**: Traditional risk assessments often fall short when adapting to new attack strategies.
- Threat Propagation**: CyberGator bridges that gap by providing insights into threat propagation and system response.
- System Under Evaluation**: Users can upload a System Under Evaluation (SUE) and safely simulate attacks and defensive actions.

At the bottom is a section titled 'Report True Risk of Vulnerabilities' with a sub-header: 'Visualize CVEs by device, software, or asset using holistic, impact-aware dashboards.'

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

The dashboard acts as the control hub for managing cybersecurity assessments and making data-driven improvements.

CVE ID	NVD Score	Node ID	Node Name
CVE-2017-8543	9.8	N00512	Server_SR12
CVE-2017-8543	9.8	N00511	Server_SR11
CVE-2013-5056	9.3	N00511	Server_SR11
CVE-2014-0301	9.3	N00511	Server_SR11
CVE-2014-0301	9.3	N00512	Server_SR12
CVE-2009-5118	9.3	N00300	Cybersecurity_Capability_Tool
CVE-2013-5056	9.3	N00512	Server_SR12
CVE-2023-20269	9.1	N40000	Firewall
CVE-2023-0101	8.8	N00300	Cybersecurity_Capability_Tool
CVE-2022-37401	8.8	N10601	Engineering_Production_Workst...

6

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

The CyberGator Dashboard provides an overview of your system's current overall Resilience Score.

- Resilience Score: A numerical representation of your system's ability to withstand and recover from cyber threats.
- Recent Events: Displays updates related to system changes, environmental risk adjustments, and attack simulations.
- Quick Navigation: Links to core functionalities such as System Tables, Simulations, and Environmental Factors.

The dashboard acts as the control hub for managing cybersecurity assessments and making data-driven improvements.

System Resilience Score

The system's current resilience score represented in a pie chart.

Overall Resilience Score [Download plot as a.png](#)

CVE ID	NVD Score	Node ID	Node Name
CVE-2017-8543	9.8	N00512	Server_SR12
CVE-2017-8543	9.8	N00511	Server_SR11
CVE-2013-5056	9.3	N00511	Server_SR11
CVE-2014-0301	9.3	N00511	Server_SR11
CVE-2014-0301	9.3	N00512	Server_SR12
CVE-2009-5118	9.3	N00300	Cybersecurity_Capability_Tool
CVE-2013-5056	9.3	N00512	Server_SR12
CVE-2023-20269	9.1	N40000	Firewall
CVE-2023-0101	8.8	N00300	Cybersecurity_Capability_Tool
CVE-2022-37401	8.8	N10601	Engineering_Production_Workst.

7

Click "System Tables" to view the system tables

System Resilience Score: 8.6004%

CyberGators

Welcome samsoncarter! You are logged in.

Dashboard Overview

The CyberGator Dashboard provides an overview of your system's current overall Resilience Score.

- Resilience Score: A numerical representation of your system's ability to withstand and recover from cyber threats.
- Recent Events: Displays updates related to system changes, environmental risk adjustments, and attack simulations.
- Quick Navigation: Links to core functionalities such as System Tables, Simulations, and Environmental Factors.

The dashboard acts as the control hub for managing cybersecurity assessments and making data-driven improvements.

System Resilience Score

The system's current resilience score represented in a pie chart.

Overall Resilience Score

CVE ID	NVD Score	Node ID	Node Name
CVE-2017-8543	9.8	N00512	Server_SR12
CVE-2017-8543	9.8	N00511	Server_SR11
CVE-2013-5056	9.3	N00511	Server_SR11
CVE-2014-0301	9.3	N00511	Server_SR11
CVE-2014-0301	9.3	N00512	Server_SR12
CVE-2009-5118	9.3	N00300	Cybersecurity_Capability_Tool
CVE-2013-5056	9.3	N00512	Server_SR12
CVE-2023-20269	9.1	N40000	Firewall
CVE-2023-0101	8.8	N00300	Cybersecurity_Capability_Tool
CVE-2022-37401	8.8	N10601	Engineering_Production_Workst.

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

System Resilience Score: 8.6004%

CyberGators

System Tables

System Tables store and organize essential data related to the system's cyber resilience.

Users can view, add, update, and remove entries, ensuring system configurations are accurately reflected for analysis.

Nodes	CVEs
List of system nodes and associated CVEs. View Table	All CVEs found in the system with their NVD scores. View Table
Software Nodes	Critical Functions
List of software nodes and their details. View Table	List of Critical Functions. View Table
Unique Software	Coming Soon

- 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

Node ID	Node Name	Node Type	Count	Avg Score	Action
N00100	System_Administrator_Terminal	Workstation	0	0	View
N00200	Virtualization_Manager_Server	Server	3	5.6	View
N00201	Virtualization_Manager_SAN	SAN	3	6.9	View
N00300	Cybersecurity_Capability_Tools_Server	Server	11	9.3	View
N00301	Cybersecurity_Capability_Tools_SAN	SAN	1	4.9	View
N00302	Cybersecurity_Capability_Tools_SAN_Archive	SAN Archive	1	4.9	View
N00303	Cybersecurity_Capability_Tools_SAN_Archive_Backup	SAN Archive Backup	1	4.9	View
N00400	Audit_Log_Server	Server	1	4.9	View
N00401	Audit_Log_SAN	SAN	1	4.9	View
N00501	Server_SR1	Server	3	5.6	View
N00502	Server_SR2	Server	3	5.6	View
N00503	Server_SR3	Server	1	4.9	View
N00504	Server_SR4	Server	1	4.9	View
N00505	Server_SR5	Server	3	6.9	View
N00506	Server_SR6	Server	3	6.9	View

Add New Node

<input type="text" value="Node ID"/>	<input type="text" value="Node Name"/>	<input type="text" value="Node Type"/>	Add Node
--------------------------------------	--	--	--------------------------

10

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

System Resilience Score: 8.6004%

CyberGators

Nodes Table

Node ID	Node Name	Node Type	Total CVEs	Max NVD Score
N00100	System_Administrator_Terminal	Workstation	0	0
N00200	Virtualization_Manager_Server	Server	3	5.6
N00201	Virtualization_Manager_SAN	SAN	3	6.9
N00300	Cybersecurity_Capability_Tools_Server	Server	11	9.3
N00301	Cybersecurity_Capability_Tools_SAN	SAN	1	4.9
N00302	Cybersecurity_Capability_Tools_SAN_Archive	SAN Archive	1	4.9
N00303	Cybersecurity_Capability_Tools_SAN_Archive_Backup	SAN Archive Backup	1	4.9
N00400	Audit_Log_Server	Server	1	4.9
N00401	Audit_Log_SAN	SAN	1	4.9
N00501	Server_SR1	Server	3	5.6
N00502	Server_SR2	Server	3	5.6

11

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

System Resilience Score: 8.6004%

CyberGators

System Tables

System Tables store and organize essential data related to the system's cyber resilience.

Users can view, add, update, and remove entries, ensuring system configurations are accurately reflected for analysis.

Nodes
List of system nodes and associated CVEs.

[View Table](#)

CVEs
All CVEs found in the system with their NVD scores.

[View Table](#)

Software Nodes
List of software nodes and their details.

[View Table](#)

Critical Functions
List of Critical Functions.

[View Table](#)

Unique Software

Coming Soon

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.

The screenshot shows a left sidebar with navigation links: Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area displays a table of 12 rows, each containing a checkbox, a CVE ID, an NVD Score, a Software ID, and a red 'X' icon. Below the table is a search bar with fields for 'CVE ID', 'NVD Score', 'Select Software Make', and 'Select Software Version', along with an 'Add CVE' button.

<input type="checkbox"/>	CVE-2015-7833	4.9	N00508	Server_SR8	X
<input type="checkbox"/>	CVE-2015-7833	4.9	N00509	Server_SR9	X
<input type="checkbox"/>	CVE-2015-7833	4.9	N00510	Server_SR10	X
<input type="checkbox"/>	CVE-2017-8543	9.8	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2014-0301	9.3	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2014-0323	6.6	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2014-0315	6.9	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2013-5058	6.9	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2013-5056	9.3	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2017-8543	9.8	N00512	Server_SR12	X
<input type="checkbox"/>	CVE-2014-0301	9.3	N00512	Server_SR12	X
<input type="checkbox"/>	CVE-2014-0323	6.6	N00512	Server_SR12	X
<input type="checkbox"/>	CVE-2014-0315	6.9	N00512	Server_SR12	X

13

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

The screenshot shows the same interface as the previous step, but the 'Select Software Make' dropdown in the 'Add New CVE' form is highlighted with an orange circle. The table and other UI elements remain identical to the previous screenshot.

<input type="checkbox"/>	CVE-2015-7833	4.9	N00508	Server_SR8	X
<input type="checkbox"/>	CVE-2015-7833	4.9	N00509	Server_SR9	X
<input type="checkbox"/>	CVE-2015-7833	4.9	N00510	Server_SR10	X
<input type="checkbox"/>	CVE-2017-8543	9.8	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2014-0301	9.3	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2014-0323	6.6	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2014-0315	6.9	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2013-5058	6.9	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2013-5056	9.3	N00511	Server_SR11	X
<input type="checkbox"/>	CVE-2017-8543	9.8	N00512	Server_SR12	X
<input type="checkbox"/>	CVE-2014-0301	9.3	N00512	Server_SR12	X
<input type="checkbox"/>	CVE-2014-0323	6.6	N00512	Server_SR12	X
<input type="checkbox"/>	CVE-2014-0315	6.9	N00512	Server_SR12	X

14

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

The screenshot shows the CyberGators application interface. At the top, it displays the System Resilience Score: 8.6004% and the title CyberGators. On the left, there's a sidebar with various navigation options like Home, Dashboard, System Tables (which is selected and highlighted in blue), System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main content area is titled 'CVEs Table'. It features a search bar labeled 'Search CVEs...' and a table with columns: CVE ID, NVD Score, Node ID, Node Name, and Remove. The 'Remove' column contains a red 'X' icon in each row. The first row, which corresponds to the highlighted 'Remove' button, is circled in red.

CVE ID	NVD Score	Node ID	Node Name	Remove
CVE-2012-2697	4.9	N00200	Virtualization_Manager_Server	X
CVE-2012-3440	5.6	N00200	Virtualization_Manager_Server	X
CVE-2010-0727	4.9	N00200	Virtualization_Manager_Server	X
CVE-2013-1935	5.7	N00201	Virtualization_Manager_SAN	X
CVE-2013-2224	6.9	N00201	Virtualization_Manager_SAN	X
CVE-2013-2188	4.7	N00201	Virtualization_Manager_SAN	X
CVE-2024-23675	6.5	N00300	Cybersecurity_Capability_Tools_Server	X
CVE-2024-23676	3.5	N00300	Cybersecurity_Capability_Tools_Server	X
CVE-2023-40593	7.5	N00300	Cybersecurity_Capability_Tools_Server	X
CVE-2023-40592	6.1	N00300	Cybersecurity_Capability_Tools_Server	X
CVE-2023-0101	8.8	N00300	Cybersecurity_Capability_Tools_Server	X

15

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

The screenshot shows the System Tables page. On the left, there's a sidebar with options: Home, Dashboard, System Tables (selected), System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main content area is titled 'System Tables' and contains several cards: 'Nodes' (List of system nodes and associated CVEs), 'CVEs' (All CVEs found in the system with their NVD scores), 'Software Nodes' (List of software nodes and their details), 'Critical Functions' (List of Critical Functions), 'Unique Software' (View and manage all unique software entries), and 'Coming Soon' (Reserved for future software management tools). The 'View Table' button under the 'Software Nodes' card is circled in red.

System Tables

System Tables store and organize essential data related to the system's cyber resilience.

Users can view, add, update, and remove entries, ensuring system configurations are accurately reflected for analysis.

Nodes
List of system nodes and associated CVEs.
[View Table](#)

CVEs
All CVEs found in the system with their NVD scores.
[View Table](#)

Software Nodes
List of software nodes and their details.
[View Table](#)

Critical Functions
List of Critical Functions.
[View Table](#)

Unique Software
View and manage all unique software entries.
[View Table](#)

Coming Soon
Reserved for future software management tools.
[View Table](#)

16

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

A screenshot of a software application interface showing a table titled "Software Nodes". The table has columns for Category, Rack Name, Node ID, Node Name, Is In Use, Software ID, Software Make, and Revision. The data includes various server components like Virtualization Managers, Cybersecurity Tools, and Audit Logs across different racks (boundary defense racks and server racks). A specific row for "Server_SR4" is highlighted with a red circle.

Category	Rack Name	Node ID	Node Name	Is In Use	Software ID	Software Make	Revision
filter d							
rack	boundary_defense_rack	N00200	Virtualization_Manager_Server	true	SW001	RedHat	R1
rack	boundary_defense_rack	N00201	Virtualization_Manager_SAN	true	SW002	RedHat	R1
rack	boundary_defense_rack	N00300	Cybersecurity_Capability_Tools_Server	true	SW006	Splunk	E1
rack	boundary_defense_rack	N00300	Cybersecurity_Capability_Tools_Server	true	SW005	Tenable	N1
rack	boundary_defense_rack	N00300	Cybersecurity_Capability_Tools_Server	true	SW003	RedHat	R1
rack	boundary_defense_rack	N00300	Cybersecurity_Capability_Tools_Server	true	SW004	McAfee	V1
rack	boundary_defense_rack	N00301	Cybersecurity_Capability_Tools_SAN	true	SW003	RedHat	R1
rack	bulk_data_storage_rack	N00302	Cybersecurity_Capability_Tools_SAN_Archive	true	SW003	RedHat	R1
rack	bulk_data_storage_rack	N00303	Cybersecurity_Capability_Tools_SAN_Archive_Backup	true	SW003	RedHat	R1
rack	boundary_defense_rack	N00400	Audit_Log_Server	true	SW003	RedHat	R1
rack	boundary_defense_rack	N00401	Audit_Log_SAN	true	SW003	RedHat	R1
rack	server_rack	N00501	Server_SR1	true	SW001	RedHat	R1
rack	server_rack	N00502	Server_SR2	true	SW001	RedHat	R1
rack	server_rack	N00503	Server_SR3	true	SW003	RedHat	R1
rack	server_rack	N00504	Server_SR4	true	SW003	RedHat	R1

17

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

A screenshot of a web-based management interface titled "System Tables". The page provides an overview of system configurations and critical functions. It features several tiles:

- Nodes:** List of system nodes and associated CVEs. Includes a "View Table" button.
- CVEs:** All CVEs found in the system with their NVD scores. Includes a "View Table" button.
- Software Nodes:** List of software nodes and their details. Includes a "View Table" button.
- Critical Functions:** List of Critical Functions. Includes a "View Table" button, which is highlighted with a red circle.
- Unique Software:** View and manage all unique software entries. Includes a "View Table" button.
- Coming Soon:** Reserved for future software management tools. Includes a "View Table" button.

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

The screenshot shows a table of critical functions with columns: ID, Work Area, Criticality, Impact Score, and a delete icon (green 'X'). A red circle highlights the delete icon for function F16. Below the table is a modal titled 'Add New Function' with dropdowns for 'Select Work Area' and 'Select Criticality', and a green 'Add Function' button.

ctors	F04	Test_Engineering	High	3	X
	F05	IT_Cybersecurity	High	3	X
	F06	IT_Cybersecurity	High	3	X
	F07	Engineering_Production	Medium	2	X
	F08	Test_Engineering	Medium	2	X
	F09	Test_Engineering	Medium	2	X
	F10	Company_Management	Medium	2	X
	F11	Engineering_Production	Low	1	X
	F12	Test_Engineering	Low	1	X
	F13	Company_Management	Low	1	X
	F14	Company_Management	Low	1	X
	F15	Company_Management	Low	1	X
ence	F16	IT_Cybersecurity	High	3	X
raph	F18	IT_Cybersecurity	High	3	X

Add New Function

Select Work Area Select Criticality Add Function

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

The screenshot shows a table of critical functions with columns: ID, Work Area, Criticality, Impact Score, and a delete icon (green 'X'). A red circle highlights the 'Select Work Area' dropdown for function F16. Below the table is a modal titled 'Add New Function' with dropdowns for 'Select Work Area' and 'Select Criticality', and a green 'Add Function' button.

Home	F03	Engineering_Production	High	3	X
Dashboard	F04	Test_Engineering	High	3	X
System Tables	F05	IT_Cybersecurity	High	3	X
System Graph	F06	IT_Cybersecurity	High	3	X
Environmental Factors	F07	Engineering_Production	Medium	2	X
Work Stations	F08	Test_Engineering	Medium	2	X
APT Simulation	F09	Test_Engineering	Medium	2	X
CVE Simulation	F10	Company_Management	Medium	2	X
FSM Simulation	F11	Engineering_Production	Low	1	X
Neo4j Graph	F12	Test_Engineering	Low	1	X
	F13	Company_Management	Low	1	X
	F14	Company_Management	Low	1	X
	F15	Company_Management	Low	1	X
	F16	IT_Cybersecurity	High	3	X

Add New Function

Select Work Area Select Criticality Add Function

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

The screenshot shows the Resilience Management System interface. On the left, there is a sidebar with various navigation options: Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area displays a table of functions (F04-F16) categorized by work area (IT Cybersecurity, Engineering_Production, Test_Engineering, Company_Management) and criticality levels (High, Medium, Low). The 'Add New Function' dialog is open at the bottom, featuring dropdown menus for 'Select Work Area' (Engineering Production, IT Cybersecurity, Test Engineering, Company Management) and 'Select Criticality' (High, Medium, Low), and a green 'Add Function' button.

Function ID	Work Area	Criticality	Value	Action
F04	Test_Engineering	High	3	X
F05	IT_Cybersecurity	High	3	X
F06	IT_Cybersecurity	High	3	X
F07	Engineering_Production	Medium	2	X
F08	Test_Engineering	Medium	2	X
F09	Test_Engineering	Medium	2	X
F10	Company_Management	Medium	2	X
F11	Engineering_Production	Low	1	X
F12	Test_Engineering	Low	1	X
F13	Company_Management	Low	1	X
F14	Company_Management	Low	1	X
F15	Company_Management	Low	1	X
F16	IT_Cybersecurity	High	3	X

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

The screenshot shows the Resilience Management System interface. The 'Add New Function' dialog is open at the bottom, featuring dropdown menus for 'Select Work Area' (Engineering Production, IT Cybersecurity, Test Engineering, Company Management) and 'Select Criticality' (High, Medium, Low). The 'High (Value: 3)' option is selected and highlighted with a blue background. The 'Add Function' button is green and has a circular orange highlight around it. The main area displays the same table of functions (F04-F16) as the previous screenshot, with the 'Add New Function' dialog overlaying the bottom portion of the screen.

Function ID	Work Area	Criticality	Value	Action
F04	Test_Engineering	High	3	X
F05	IT_Cybersecurity	High	3	X
F06	IT_Cybersecurity	High	3	X
F07	Engineering_Production	Medium	2	X
F08	Test_Engineering	Medium	2	X
F09	Test_Engineering	Medium	2	X
F10	Company_Management	Medium	2	X
F11	Engineering_Production	Low	1	X
F12	Test_Engineering	Low	1	X
F13	Company_Management	Low	1	X
F14	Company_Management	Low	1	X
F15	Company_Management	Low	1	X
F16	IT_Cybersecurity	High	3	X

22

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

System Resilience Score: 8.6004%

CyberGators

System Critical Functions Table

Function Number	Work Area	Criticality	Criticality Value	Remove
F01	Engineering_Production	High	3	X
F02	Engineering_Production	High	3	X
F03	Engineering_Production	High	3	X
F04	Test_Engineering	High	3	X
F05	IT_Cybersecurity	High	3	X
F06	IT_Cybersecurity	High	3	X
F07	Engineering_Production	Medium	2	X
F08	Test_Engineering	Medium	2	X
F09	Test_Engineering	Medium	2	X
F10	Company_Management	Medium	2	X
F11	Engineering_Production	Low	1	X

23

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

System Resilience Score: 8.6004%

CyberGators

Node Association Manager

Assign Nodes to Function

Select Function:

Select a function

- F01 - Engineering_Production
- F02 - Engineering_Production
- F03 - Engineering_Production
- F04 - Test_Engineering
- F05 - IT_Cybersecurity
- V F06 - IT Cybersecurity

Select Node:

Select a node to view its functions

Functions assigned to this node:

Function Number	Work Area	Criticality

24

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

The screenshot shows the Node Association Manager page. At the top, it displays "System Resilience Score: 8.6004%" and the title "Node Association Manager". Below the title are buttons for "Back to Critical Functions", "Refresh Data", and "Reset Node Associations". The main area is titled "Assign Nodes to Function" and shows "Select Function: F03 - Engineering_Production". A list of assigned nodes is displayed, including "Server_SR1 (N00501)", "Engineering_Production_SAN_1 (N00611)", "Engineering_Production_SAN_Archive_1 (N00612)", "Engineering_Production_SAN_2 (N00621)", "Engineering_Production_SAN_Archive_2 (N00622)", and "Engineering_Production_Workstation_2 (N10602)". A vertical scroll bar is visible on the right side of this list. Below the assigned nodes, there is a list of available nodes: "System_Administrator_Terminal (N00100)", "Virtualization_Manager_Server (N00200)", "Virtualization_Manager_SAN (N00201)", "Cybersecurity_Capability_Tools_Server (N00300)", "Cybersecurity_Capability_Tools_SAN (N00301)", and "Cybersecurity Capability Tools SAN Archive (N00302)". At the bottom, there is a table titled "Functions assigned to this node:" with columns for "Function Number", "Work Area", and "Criticality".

25

Click "Update Node Assignments"

The screenshot shows the Node Association Manager page with the "Update Node Assignments" button highlighted by a red circle. The left sidebar contains navigation links: Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area is titled "Node Association Manager" and shows the same "Assign Nodes to Function" section as the previous screenshot. The "Update Node Assignments" button is now prominent at the bottom of the list of assigned nodes. Below it, the "View Functions by Node" section and the "Functions assigned to this node:" table are visible.

26

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

The screenshot shows the 'Node Association Manager' interface. On the left, a sidebar menu includes options like Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area is titled 'NODE ASSOCIATION MANAGER'. It has two sections: 'Assign Nodes to Function' and 'View Functions by Node'. In the 'Assign Nodes to Function' section, 'Select Function:' is set to 'F03 - Engineering_Production' and 'Assign Nodes:' lists several nodes. In the 'View Functions by Node' section, 'Select Node:' dropdown is open, showing a list of nodes including 'Cybersecurity_Capability_Tools_SAN_Archive_Backup (N00303)', which is highlighted with a red circle. Other nodes listed are Audit_Log_Server (N00400), Audit_Log_SAN (N00401), Server_SR1 (N00501), Server_SR2 (N00502), and Server_SR3 (N00503).

27

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

The screenshot shows the 'Node Association Manager' interface. The sidebar and top navigation are identical to the previous screenshot. The main area shows the 'Assign Nodes to Function' and 'View Functions by Node' sections. In the 'View Functions by Node' section, 'Select Node:' is set to 'System_Administrator_Terminal (N00100)'. Below this, a 'Node Details' block provides information: Node ID: N00100, Node Name: System_Administrator_Terminal, Node Type: Workstation, Risk Factor: Medium, Critical Data Stored: False, and Redundancy: False. A red circle highlights the 'Functions assigned to this node:' heading. A table below lists the assigned functions:

Function Number	Work Area	Criticality
F05	IT_Cybersecurity	High
F06	IT_Cybersecurity	High

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

The screenshot shows the CyberGators Node Association Manager interface. On the left, a blue sidebar menu lists various system components like Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, and Neo4j Graph. Below these are two buttons: 'Reset Options' and 'Recalculate Resilience'. The main content area has an orange header with the resilience score 'System Resilience Score: 8.6004%' and the title 'CyberGators'. Below the header is the 'Node Association Manager' section. It contains a sub-section 'Assign Nodes to Function' where 'F03 - Engineering_Production' is selected. A list of nodes assigned to this function includes 'Server_SR1 (N00501)', 'Engineering_Production_SAN_1 (N00611)', 'Engineering_Production_SAN_Archive_1 (N00612)', 'Engineering_Production_SAN_2 (N00621)', 'Engineering_Production_SAN_Archive_2 (N00622)', and 'Engineering_Production_Workstation_2 (N10602)'. There is a 'Update Node Assignments' button. Another sub-section 'View Functions by Node' shows 'System_Administrator_Terminal (N00100)' selected, with details 'Node ID: N00100' and 'Node Name: System_Administrator_Terminal'. At the top right are 'Refresh Data' and 'Reset Node' buttons.

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

The screenshot shows the CyberGators System Critical Functions Table interface. The top navigation bar includes the resilience score 'System Resilience Score: 8.6004%', the title 'CyberGators', and a 'Logout' button. Below the navigation is a sub-navigation bar with 'Go to System Tables' and 'Manage Node Associations' buttons. A 'Reset Functions Table' button is highlighted with a yellow circle. The main content is a table titled 'System Critical Functions Table'. The table has columns: 'Function Number', 'Work Area', 'Criticality', 'Criticality Value', and 'Remove'. The rows list critical functions from F01 to F11, categorized by work area (Engineering_Production, Test_Engineering, IT_Cybersecurity, Company_Management) and criticality levels (High, Medium, Low). Each row includes a checkbox in the first column and a 'Remove' button in the last column. The background of the table rows transitions from red for High criticality to yellow for Low criticality.

Function Number	Work Area	Criticality	Criticality Value	Remove
F01	Engineering_Production	High	3	X
F02	Engineering_Production	High	3	X
F03	Engineering_Production	High	3	X
F04	Test_Engineering	High	3	X
F05	IT_Cybersecurity	High	3	X
F06	IT_Cybersecurity	High	3	X
F07	Engineering_Production	Medium	2	X
F08	Test_Engineering	Medium	2	X
F09	Test_Engineering	Medium	2	X
F10	Company_Management	Medium	2	X
F11	Engineering_Production	Low	1	X

30

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

The screenshot shows the 'System Tables' page with a sidebar on the left containing navigation links like Home, Dashboard, System Tables (which is selected), System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main content area displays several cards:

- Nodes**: List of system nodes and associated CVEs. **View Table** button.
- CVEs**: All CVEs found in the system with their NVD scores. **View Table** button.
- Software Nodes**: List of software nodes and their details. **View Table** button.
- Critical Functions**: List of Critical Functions. **View Table** button.
- Unique Software**: View and manage all unique software entries. **View Table** button (circled in orange).
- Coming Soon**: Reserved for future software management tools. **View Table** button.

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

The screenshot shows the 'Unique Software Table' page. At the top, there is a 'Go to System Tables' button and a search bar labeled 'Search Software...'. Below is a table with the following columns: Software ID, Make, Description, Version, and Expansion (with a '+' icon). The table contains the following data:

Software ID	Make	Description	Version	Expansion
SW001	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 5.0	+
SW002	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 6.0	+
SW006	Splunk	Enterprise Security Information and Event Manager (SIEM)	8.6	+
SW005	Tenable	Nessus Vulnerability Scanner	8.10.0	+
SW003	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 7.1	+
SW004	McAfee	VirusScan Enterprise	2	+
SW007	Microsoft	Windows Server 2008 Service Pack 2	Windows Server 2008 SP2	+
SW008	OpenOffice	Apache OpenOffice (Open Source)	4.1.1.4	+
SW009	Cisco	Catalyst 2960-X IOS	IOS 15.2(1)E	+
SW0010	Cisco	Meraki MS425-32 Layer 3 Switch (firmware 2014-09-23)	2014-09-23	+
SW0011	Cisco	FirePower 4125 Next Generation Firewall with Firepower Threat Defense (FTD) Software	6.6.7	+

At the bottom, there is a form titled 'Add New Software' with fields for Software Make, Software Description, Software Version, and a green 'Add Software' button.

32

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

The screenshot shows a software management interface with a sidebar on the left containing navigation links like Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area displays a table of software packages:

Software ID	Make	Description	Version
SW001	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 5.0
SW002	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 6.0
SW006	Splunk	Enterprise Security Information and Event Manager (SIEM)	8.6
SW005	Tenable	Nessus Vulnerability Scanner	8.10.0
SW003	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 7.1
SW004	McAfee	VirusScan Enterprise	2
SW007	Microsoft	Windows Server 2008 Service Pack 2	Windows Server 2008 SP2
SW008	OpenOffice	Apache OpenOffice (Open Source)	4.1.1.4
SW009	Cisco	Catalyst 2960-X IOS	IOS 15.2(1)E
SW010	Cisco	Meraki MS425-32 Layer 3 Switch (firmware 2014-09-23)	2014-09-23
SW011	Cisco	FirePower 4125 Next Generation Firewall with Firepower Threat Defense (FTD) Software	6.6.7

Below the table, a section titled "Details for SW001" shows node information and associated CVEs:

Nodes: N00200, N00501, N00502, N00611, N00801, N10701, N10702

CVEs: CVE-2012-2697 (NVD: 4.9), CVE-2012-3440 (NVD: 5.6), CVE-2010-0727 (NVD: 4.9), CVE-2023-47804 (NVD: 8.8), CVE-2022-37401 (NVD: 8.8), CVE-2021-33035 (NVD: 7.8), CVE-2020-13958 (NVD: 7.8), CVE-2017-12607 (NVD: 7.8)

Buttons for "Add New Software" and "Add Software" are visible at the bottom right.

33

To remove the Software from the system, click "X"

The screenshot shows a software management interface with a sidebar on the left containing navigation links like Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area displays a table of software packages:

Software ID	Make	Description	Version	Expand	Remove
SW001	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 5.0	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW002	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 6.0	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW006	Splunk	Enterprise Security Information and Event Manager (SIEM)	8.6	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW005	Tenable	Nessus Vulnerability Scanner	8.10.0	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW003	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 7.1	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW004	McAfee	VirusScan Enterprise	2	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW007	Microsoft	Windows Server 2008 Service Pack 2	Windows Server 2008 SP2	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW008	OpenOffice	Apache OpenOffice (Open Source)	4.1.1.4	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW009	Cisco	Catalyst 2960-X IOS	IOS 15.2(1)E	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW010	Cisco	Meraki MS425-32 Layer 3 Switch (firmware 2014-09-23)	2014-09-23	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>
SW011	Cisco	FirePower 4125 Next Generation Firewall with Firepower Threat Defense (FTD) Software	6.6.7	<input type="button" value="+"/>	<input style="background-color: #ff0000; color: white; border-radius: 50%;" type="button" value="X"/>

Below the table, a section titled "Details for SW001" shows node information and associated CVEs:

Nodes: N00200, N00501, N00502, N00611, N00801, N10701, N10702

CVEs: CVE-2012-2697 (NVD: 4.9), CVE-2012-3440 (NVD: 5.6), CVE-2010-0727 (NVD: 4.9), CVE-2023-47804 (NVD: 8.8), CVE-2022-37401 (NVD: 8.8), CVE-2021-33035 (NVD: 7.8), CVE-2020-13958 (NVD: 7.8), CVE-2017-12607 (NVD: 7.8)

34

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

The screenshot shows a navigation sidebar on the left with various options like Home, Dashboard, System Tables, System Graph, etc. The main area is titled 'Unique Software Table' and contains a table of installed software. At the bottom, there's an 'Add New Software' form with fields for Software Make, Software Description, and Software Version, and a green 'Add Software' button. The 'Software Make' field is highlighted with a red circle.

Software ID	Make	Description	Version
1	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 6.0
	Splunk	Enterprise Security Information and Event Manager (SIEM)	8.6
	Tenable	Nessus Vulnerability Scanner	8.10.0
	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 7.1
	McAfee	VirusScan Enterprise	2
	Microsoft	Windows Server 2008 Service Pack 2	Windows Server 2008 SP2
	OpenOffice	Apache OpenOffice (Open Source)	4.1.1.4
	Cisco	Catalyst 2960-X IOS	IOS 15.2(1)E
0	Cisco	Meraki MS425-32 Layer 3 Switch (firmware 2014-09-23)	2014-09-23
1	Cisco	FirePower 4125 Next Generation Firewall with Firepower Threat Defense (FTD) Software 6.6.7	

35

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

The screenshot shows the same interface as the previous one, but the 'Software Description' field in the 'Add New Software' form is highlighted with a red circle.

Software ID	Make	Description	Version	Expand
1	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 6.0	+
	Splunk	Enterprise Security Information and Event Manager (SIEM)	8.6	+
	Tenable	Nessus Vulnerability Scanner	8.10.0	+
	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 7.1	+
	McAfee	VirusScan Enterprise	2	+
	Microsoft	Windows Server 2008 Service Pack 2	Windows Server 2008 SP2	+
	OpenOffice	Apache OpenOffice (Open Source)	4.1.1.4	+
	Cisco	Catalyst 2960-X IOS	IOS 15.2(1)E	+
0	Cisco	Meraki MS425-32 Layer 3 Switch (firmware 2014-09-23)	2014-09-23	+
1	Cisco	FirePower 4125 Next Generation Firewall with Firepower Threat Defense (FTD) Software 6.6.7		+

36

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

Menu

- Home
- Dashboard
- System Tables
- System Graph
- Environmental Factors
- Work Stations
- APT Simulation
- CVE Simulation
- FSM Simulation
- Neo4j Graph

Reset Options ▾

Recalculate Resilience

System Resilience Score: 8.6004%

CyberGators

System Tables

System Tables store and organize essential data related to the system's cyber resilience.

Users can view, add, update, and remove entries, ensuring system configurations are accurately reflected for analysis.

Nodes	CVEs
List of system nodes and associated CVEs. View Table	All CVEs found in the system with their NVD scores. View Table
Software Nodes	Critical Functions
List of software nodes and their details. View Table	List of Critical Functions. View Table
Unique Software	Coming Soon

37

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

Menu

- Home
- Dashboard
- System Tables
- System Graph
- Environmental Factors
- Work Stations
- APT Simulation
- CVE Simulation
- FSM Simulation
- Neo4j Graph

Reset Options ▾

Recalculate Resilience

System Resilience Score: 8.6004%

CyberGators

System Graph

System Graph Overview

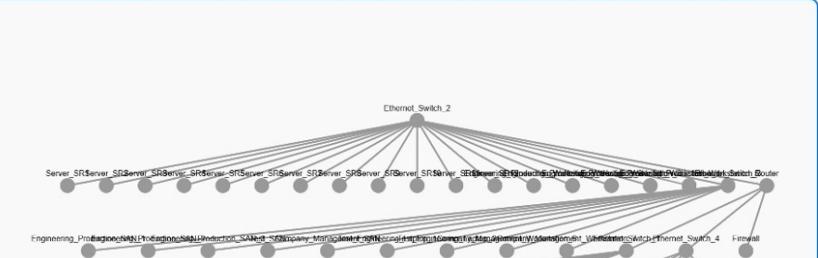
This graph visualizes the System Under Evaluation (SUE) using nodes' data.

Each node represents a system component like a server, switch, workstation, SAN, router, or firewall.

Each edge reflects a direct connection between components.

Click to See System Graph Details

Refresh Graph

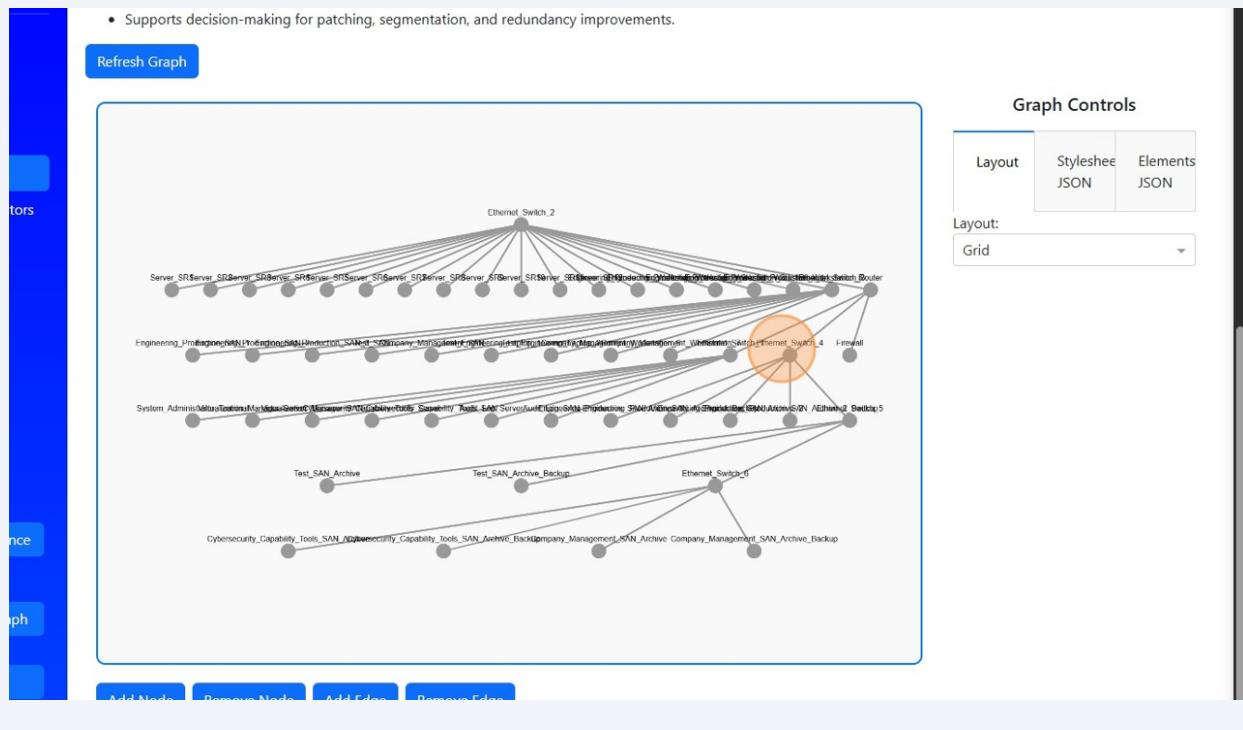


Graph Con

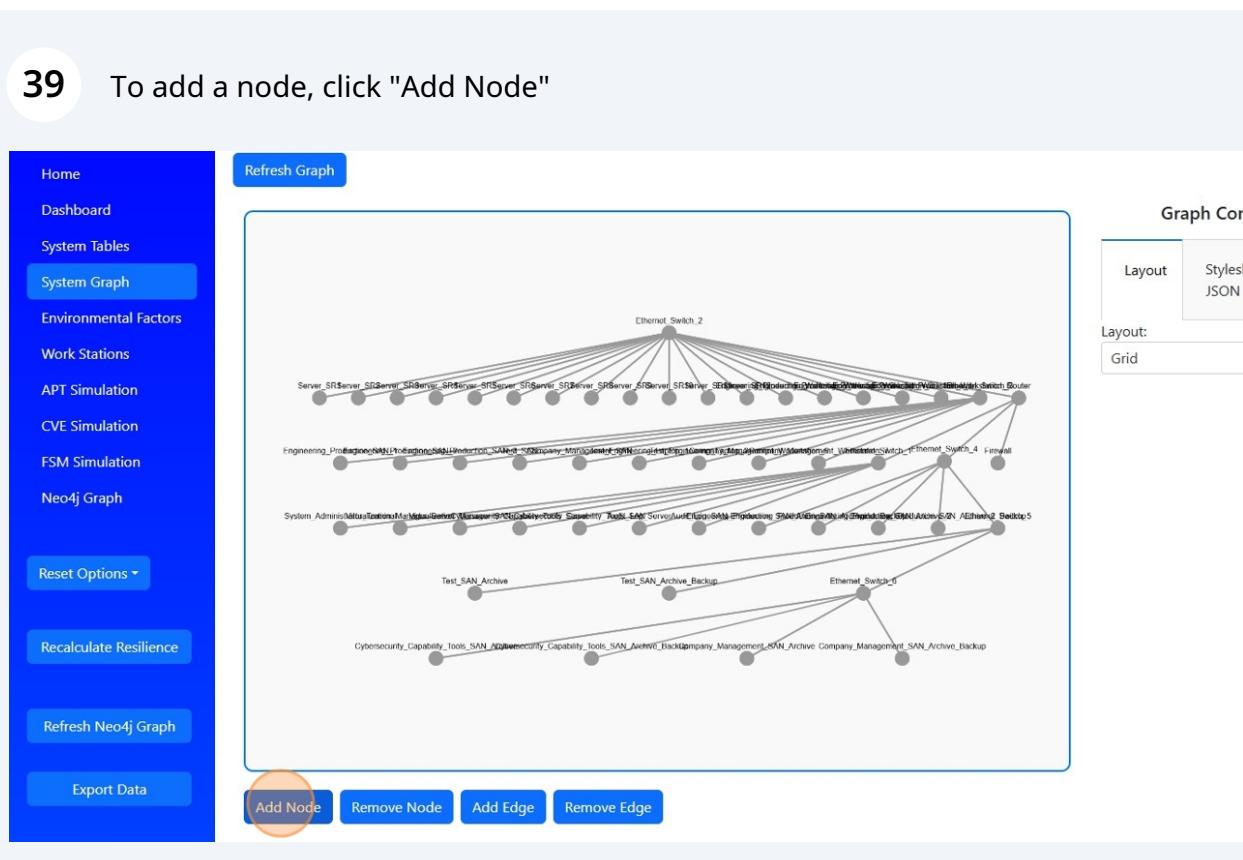
- Layout
- Styles JSON

Layout:
Grid

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

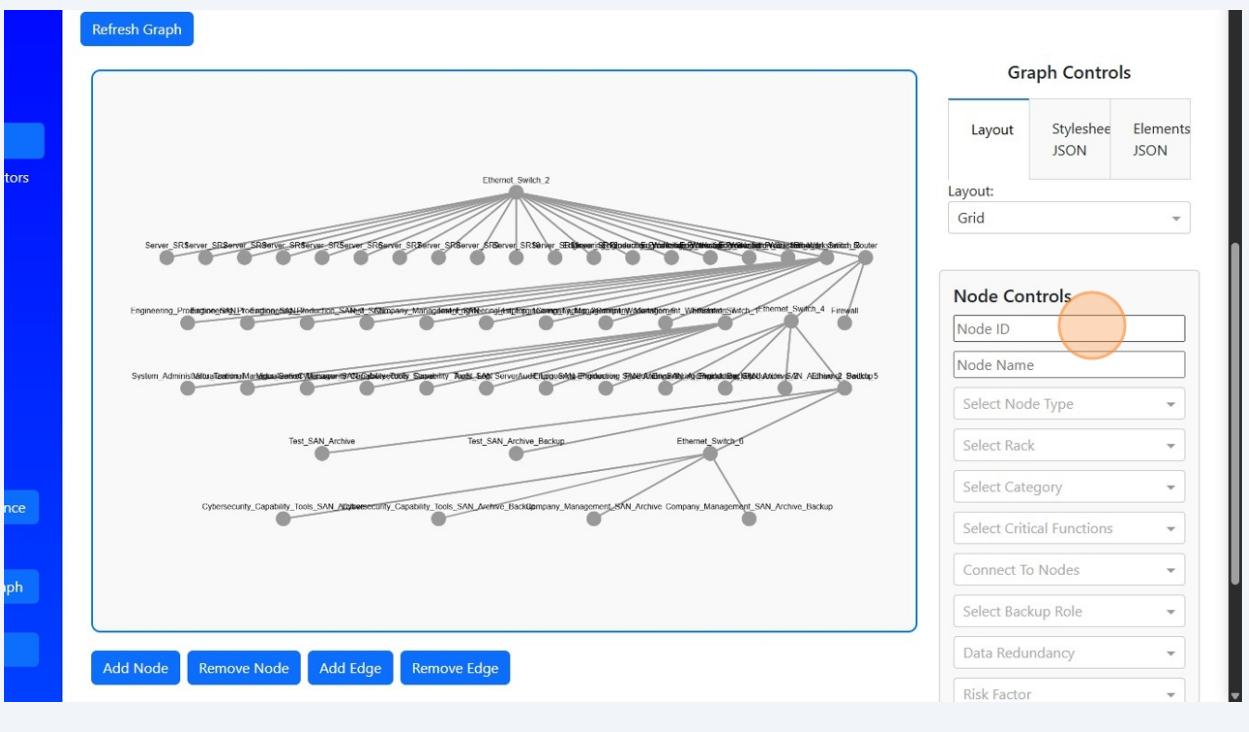


39 To add a node, click "Add Node"



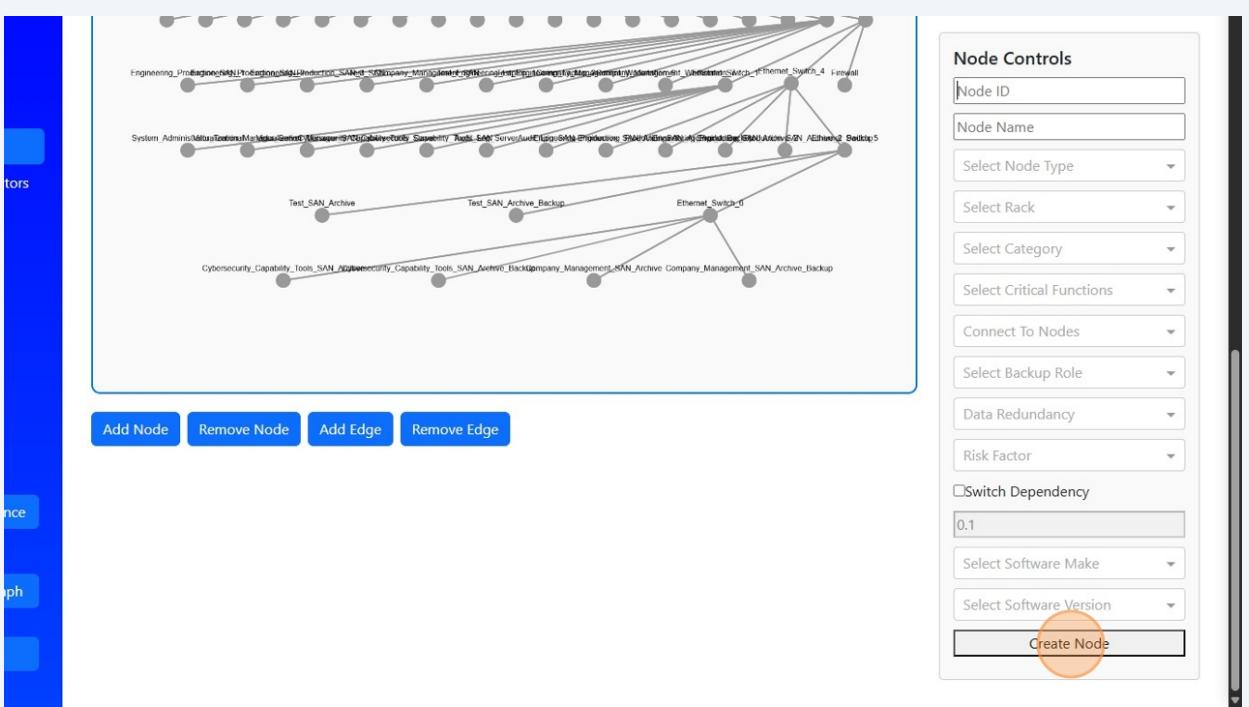
40

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.

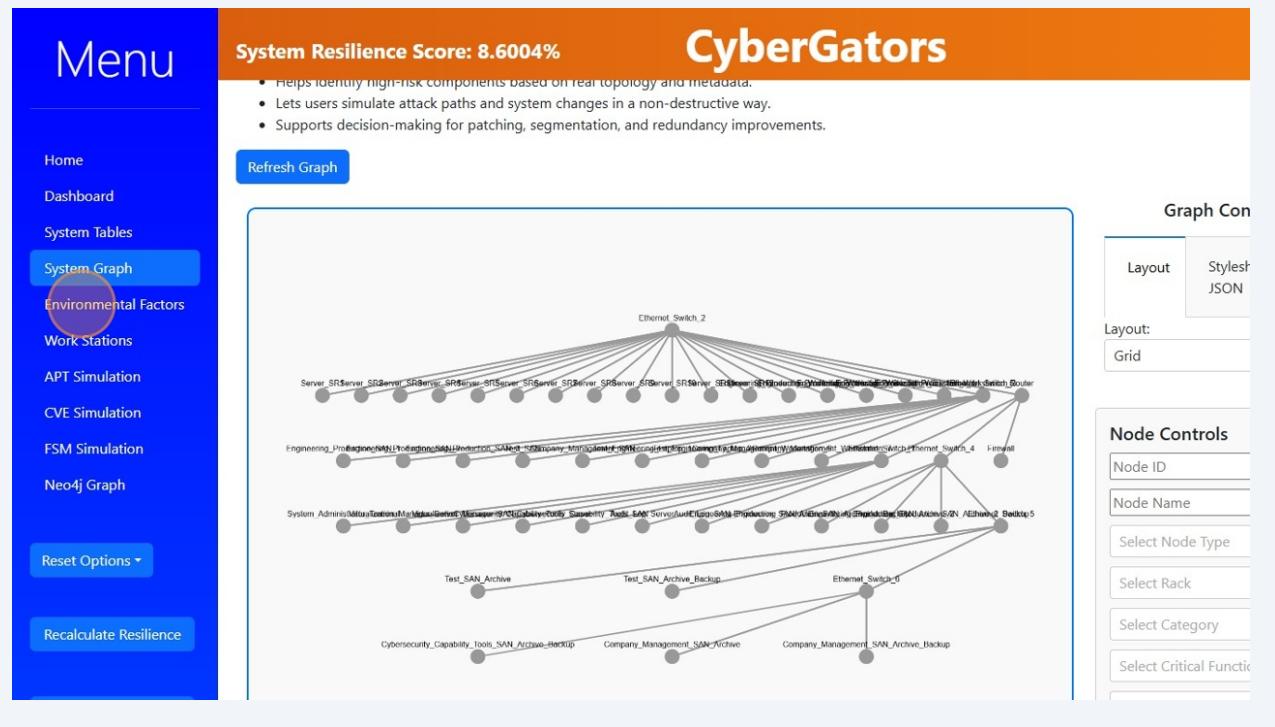
The screenshot shows a complex network graph with numerous nodes and edges. One specific node, 'Cybersecurity_Capability_Tool_SAN_Archive', is highlighted with a red circle. Below the graph, there are four buttons: 'Add Node', 'Remove Node', 'Add Edge', and 'Remove Edge'. The 'Remove Node' button is also highlighted with a red circle. To the right of the graph, there is a sidebar titled 'Node Controls' containing various configuration options like 'Node ID', 'Node Name', etc., each with its own input field. At the bottom right of the sidebar, there is a 'Create No' button.

43

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

The screenshot shows the same network graph as the previous one. The node 'Cybersecurity_Capability_Tool_SAN_Archive' is again highlighted with a red circle. Below the graph, the 'Add Edge' button is highlighted with a red circle. A message at the bottom right of the sidebar area says 'Node 'N00302' removed success'.

- 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.

The screenshot shows the 'Edit Environmental Risk Factor Weights' page. At the top, it displays the system resilience score of 8.6004% and a 'Logout' button. Below this, the title 'Edit Environmental Risk Factor Weights' is centered, with a sub-instruction 'Adjust the impact weight of each risk factor value on resilience scoring.' Three risk factors are listed in boxes: 'Flood risk', 'Unlocked doors', and 'Security guard present'. Each box contains three rows for 'Yes', 'No', and 'NA', each with a numerical input field for adjusting the weight. In the 'Flood risk' section, the 'Yes' input field is highlighted with an orange circle, indicating it is currently selected or being edited.

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

The screenshot shows the CyberGators application interface. On the left, a sidebar menu includes options like Home, Dashboard, System Tables, System Graph, Environmental Factors (which is selected and highlighted in blue), Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. In the center, there are three main configuration sections: 'Access via other room' (with 'Yes' at 0.3, 'No' at 0, and 'NA' at 0), 'It staff count' (with 'Low' at 1, 'Medium' at 0.5, 'High' at 0.1, and 'NA' at 0), and a 'Smart lock pro installed' section (with 'Yes' at 0, 'No' at 0.3, and 'NA' at 0). At the bottom right of the central area is a blue button labeled 'Save Changes' with a small icon, which is circled in orange to indicate it should be clicked.

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

This screenshot is similar to the previous one but with a key difference: the 'Work Stations' option in the sidebar menu is now highlighted with a red circle, indicating it has been selected. The rest of the interface, including the resilience score, risk factor configurations, and the 'Save Changes' button, remains the same.

48

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

The screenshot shows the CyberGators application interface. On the left, a blue sidebar menu lists various options: Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations (which is selected and highlighted in blue), APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, and Recalculate Resilience. The main content area has an orange header bar with the text "System Resilience Score: 8.6004%" and the "CyberGators" logo. Below the header, the title "Work Stations" is displayed with the sub-instruction "Explore and modify risk factors by work area." There are four tabs representing different work areas: "Engineering Production" (selected), "IT Cybersecurity" (highlighted with a red circle), "View Risk Factors" (button), "Test Engineering" (button). Another tab, "Company Management", also has a "View Risk Factors" button. A green button labeled "+ Add Work Area" is located below the tabs. At the bottom right, there is a link "▶ Change Log".

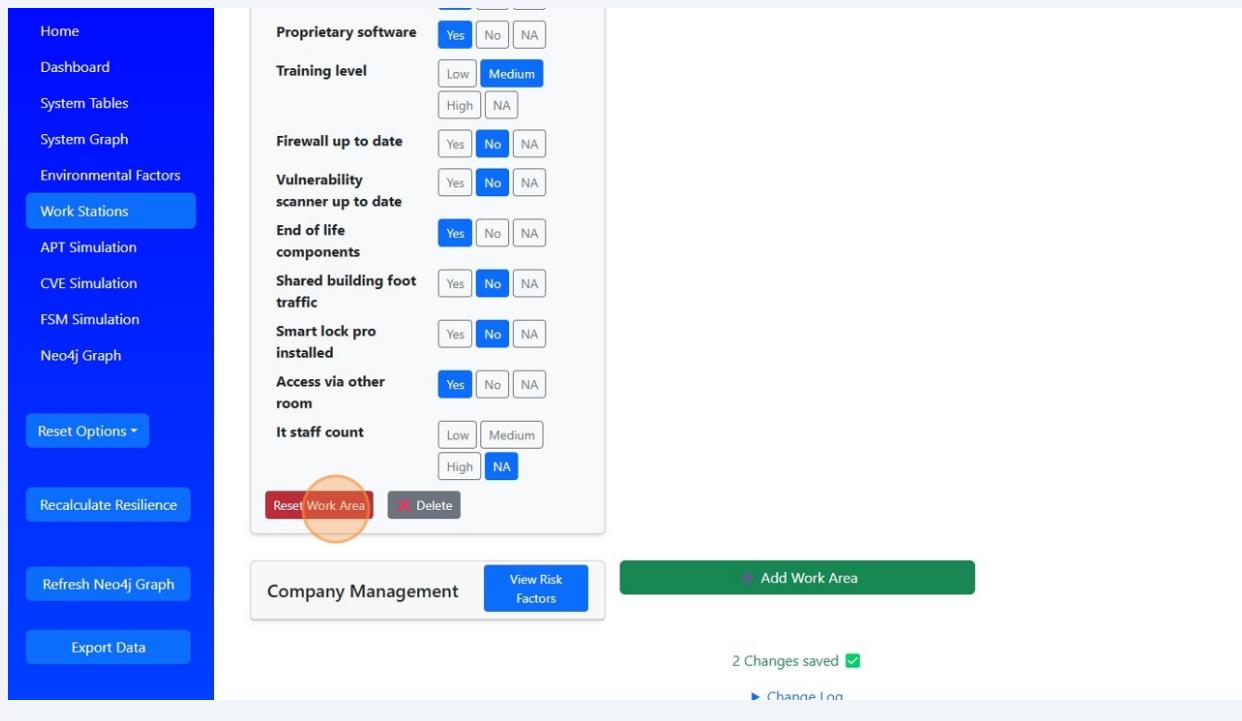
49

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

The screenshot shows the CyberGators application interface. The sidebar menu is identical to the previous screenshot. The main content area displays the "Work Stations" section with the sub-instruction "Explore and modify risk factors by work area." It shows the "Engineering Production" tab selected. Under this tab, there is a table of risk factors with three columns: the factor name, a slider scale, and three buttons ("Yes", "No", "NA"). The first row, "Flood risk", has its slider set to "Yes" and is highlighted with a red circle. Other rows include "Unlocked doors" (slider at "Yes"), "Security guard present" (slider at "Part-time"), "Alarm coverage" (slider at "Limited"), "Access control" (slider at "Low"), "Key lock usage" (slider at "Yes"), "Outdated components" (slider at "Yes"), and "Patching delays" (slider at "Yes"). To the right of the table are three tabs: "IT Cybersecurity" (selected), "View Risk Factors" (button), and "Test Engineering" (button).

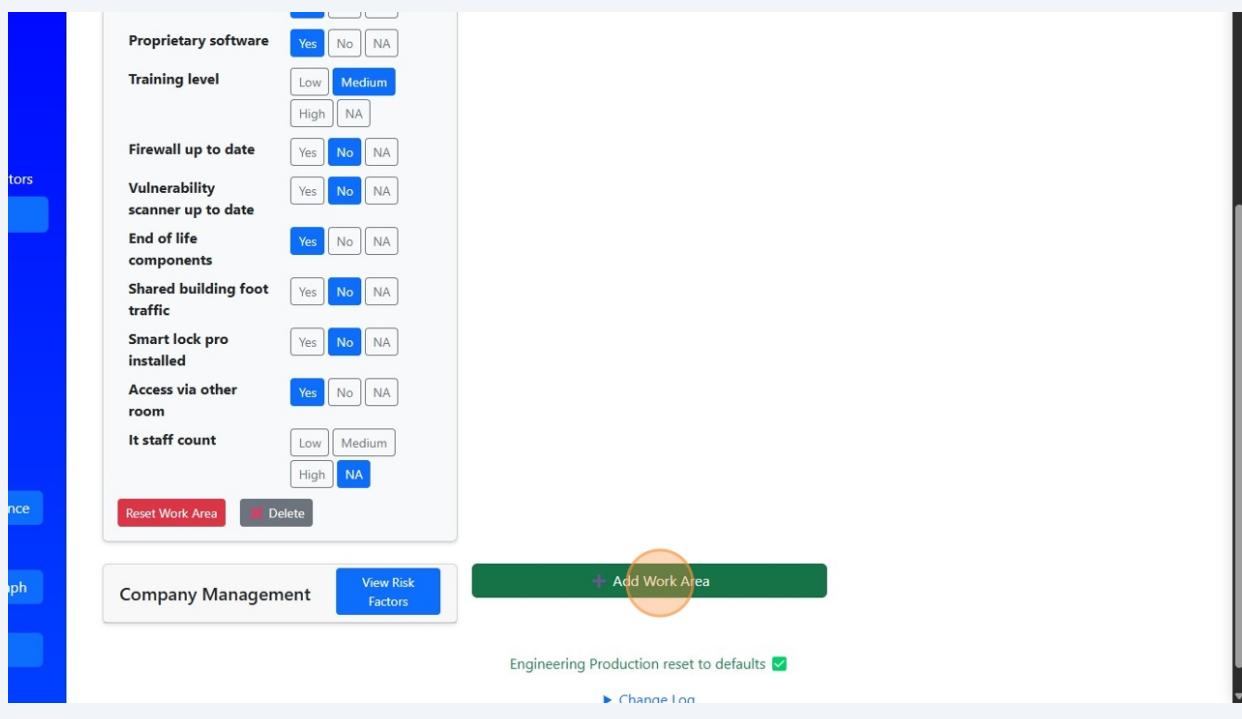
50

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



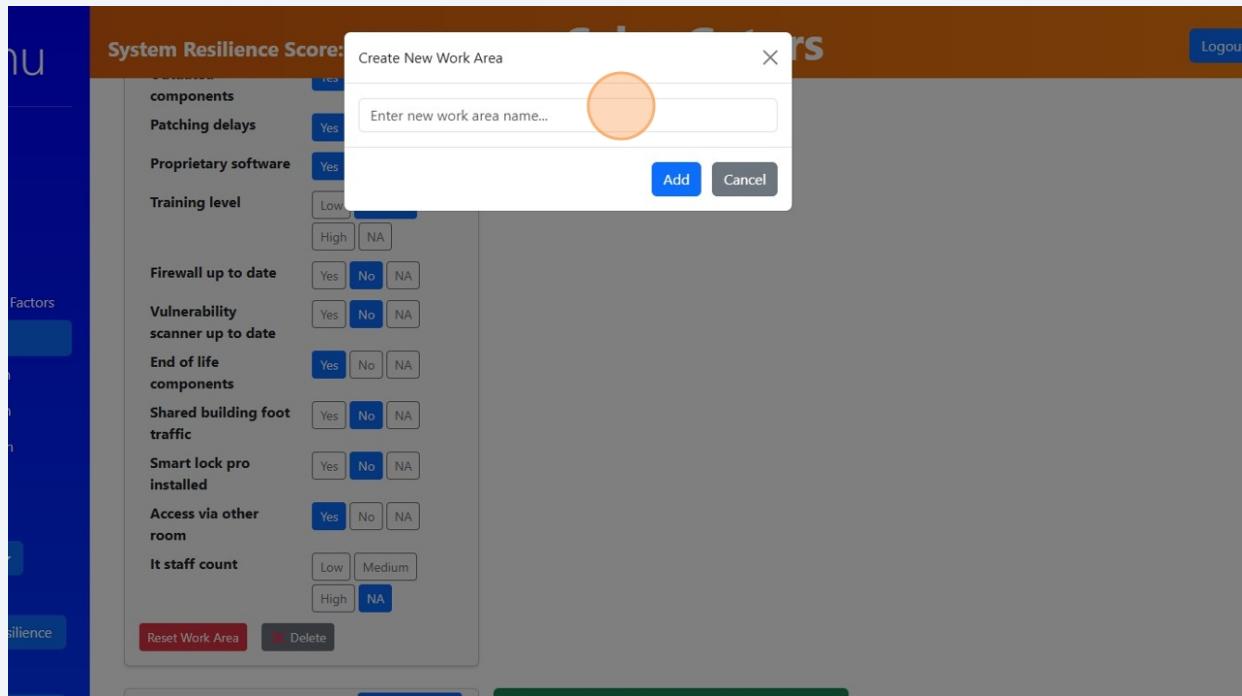
51

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"

System Resilience Score: 8.6004%

Factor	Value	Yes	No	NA
components	Yes	Yes	No	NA
Patching delays	Yes	Yes	No	NA
Proprietary software	Yes	Yes	No	NA
Training level	Low	Medium	No	NA
Firewall up to date	Yes	Yes	No	NA
Vulnerability scanner up to date	Yes	Yes	No	NA
End of life components	Yes	Yes	No	NA
Shared building foot traffic	Yes	Yes	No	NA
Smart lock pro installed	Yes	Yes	No	NA
Access via other room	Yes	Yes	No	NA
IT staff count	Low	Medium	No	NA

Company Management View Risk Add Work Area

54

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

The screenshot shows the CyberGators interface. On the left, a blue sidebar menu lists various options: Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation (which is selected), CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options, Recalculate Resilience, and Refresh Neo4j Graph. The main area is titled 'System Graph View' and displays a network graph with nodes. At the top, it says 'System Resilience Score: 8.6004%' and 'CyberGators'. Below the graph, there is a 'Fetch CVSS Metadata' button, a 'Select CVE for Attack Simulation' dropdown, and a 'Select a CVE to simulate attack propagation:' dropdown. The graph itself consists of several nodes connected by lines, with some nodes colored orange and others green.

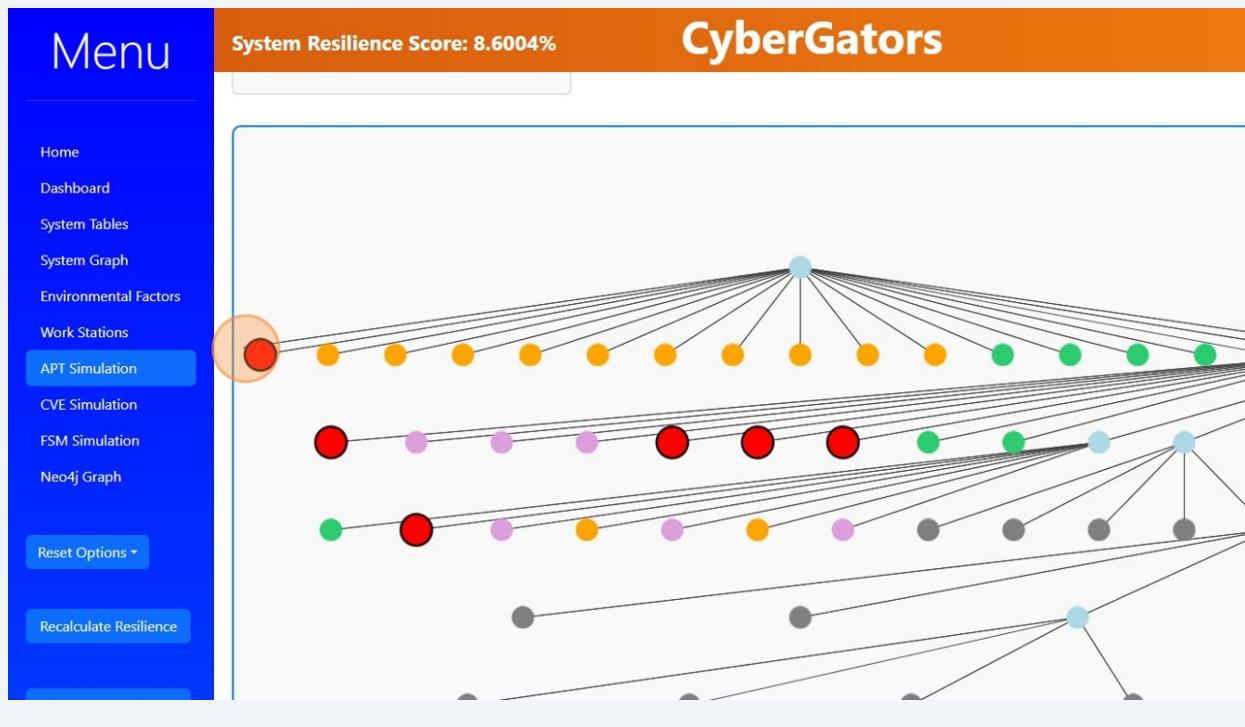
55

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

The screenshot shows the CyberGators interface again. The sidebar menu is identical to the previous one. The main area is titled 'System Graph View' and displays a network graph with nodes. The 'Select CVE for Attack Simulation' dropdown is open, showing a list of CVE entries: Select CVE..., CVE-2007-2152, CVE-2009-5118, CVE-2010-0727 (which is highlighted with a red circle), CVE-2012-2697, CVE-2012-3440, and CVE-2013-1935. Below the dropdown, the graph shows nodes connected by lines, with some nodes colored purple, green, and blue.

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.

System Resilience Score: 8.6004%

CyberGators

Node ID: N00801

Node Type: san

Critical Functions: ['F10', 'F13', 'F14', 'F15']

CVE Count: 3

Total NVD Score: 15.4

CVSS Filtering Controls

Attack Vector: ADJACENT_NETWORK, NETWORK

Privileges Required: LOW, NA, NONE

User Interaction: NA, NONE

Minimum CVSS Score: 0.1

Run Simulation

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

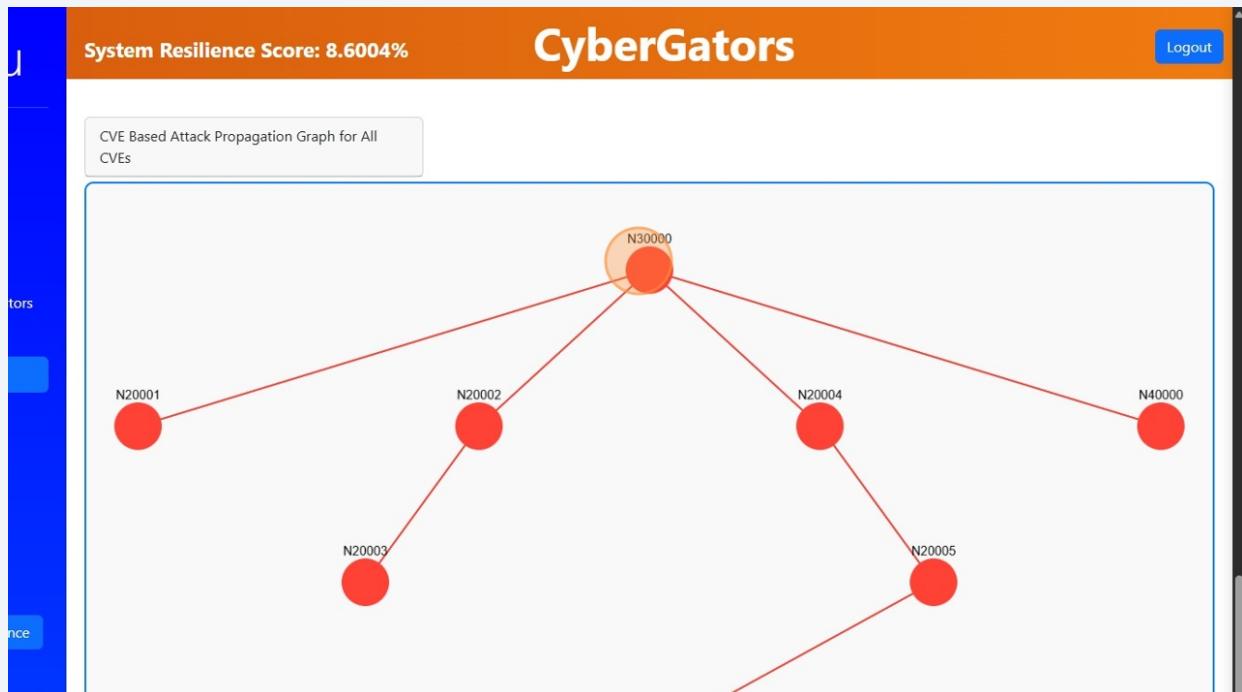
The screenshot shows the CyberGators application interface. On the left, there's a sidebar with various navigation options like Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, and several simulation buttons (APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph). Below these are buttons for Reset Options, Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area has a header 'Node Type: Sun' with metrics: Critical Functions: ['F10', 'F13', 'F14', 'F15'], CVE Count: 3, and Total NVD Score: 15.4. Below this is a 'CVSS Filtering Controls' section with dropdowns for Attack Vector (set to ADJACENT_NETWORK and NETWORK), Privileges Required (LOW, NA, NONE), User Interaction (NA, NONE), and Minimum CVSS Score (0.1). A large blue button labeled 'Run Simulation' is centered in this section and is circled in orange. Below it is a 'Simulation Results' section which is currently empty. Further down is an 'Attack Log' section with tabs for 'Entry Node' and 'Reachable Nodes'. At the bottom, a box displays 'CVE Based Attack Propagation Graph for All CVEs'.

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

This screenshot shows the same CyberGators interface as the previous one, but after a simulation has been run. The 'Run Simulation' button is still highlighted with an orange circle. In the 'Simulation Results' section, a message 'No entry nodes passed the CVSS filter.' is displayed in red. The 'Attack Log' section shows three entries corresponding to different CVEs: 'N40000 (Firewall) - CVE-2023-20269', 'N40000 (Firewall) - CVE-2023-20256', and 'N40000 (Firewall) - CVE-2023-20247'. Each entry lists the 'Entry Node' and 'Reachable Nodes' for that specific CVE, showing a list of nodes and their scores. The overall resilience score at the top is 8.6004%.

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.

The screenshot shows the CyberGators application interface with the "APT Simulation" menu item selected in the sidebar. The main area displays a network graph with several nodes. One node, N20004, is highlighted with a yellow/orange glow, indicating it is selected. Below the graph, a detailed information box is displayed for this selected node:

Node Name:	Ethernet_Switch_4
Node ID:	N20004
Type:	switch
CVEs:	4
Total CVE Score:	24.1
Critical Functions:	F16
Privilege:	N/A
Rack:	N/A

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

Node Name: Ethernet_Switch_4
Node ID: N20004
Type: switch
CVEs: 4
Total CVE Score: 24.1
Critical Functions: F16
Privilege: N/A
Rack: N/A

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

CVE ID	Nodes Affected	Impact Score	Patch
CVE-2015-7833	22	107.8	Patch
CVE-2023-47804	9	79.2	Patch
CVE-2022-37401	9	79.2	Patch
CVE-2021-33035	9	70.2	Patch
CVE-2017-12607	9	70.2	Patch
CVE-2020-13958	9	70.2	Patch
CVE-2013-2224	10	69	Patch
CVE-2013-1935	10	57	Patch
CVE-2013-2188	10	47	Patch
CVE-2012-3440	7	39.2	Patch

64

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

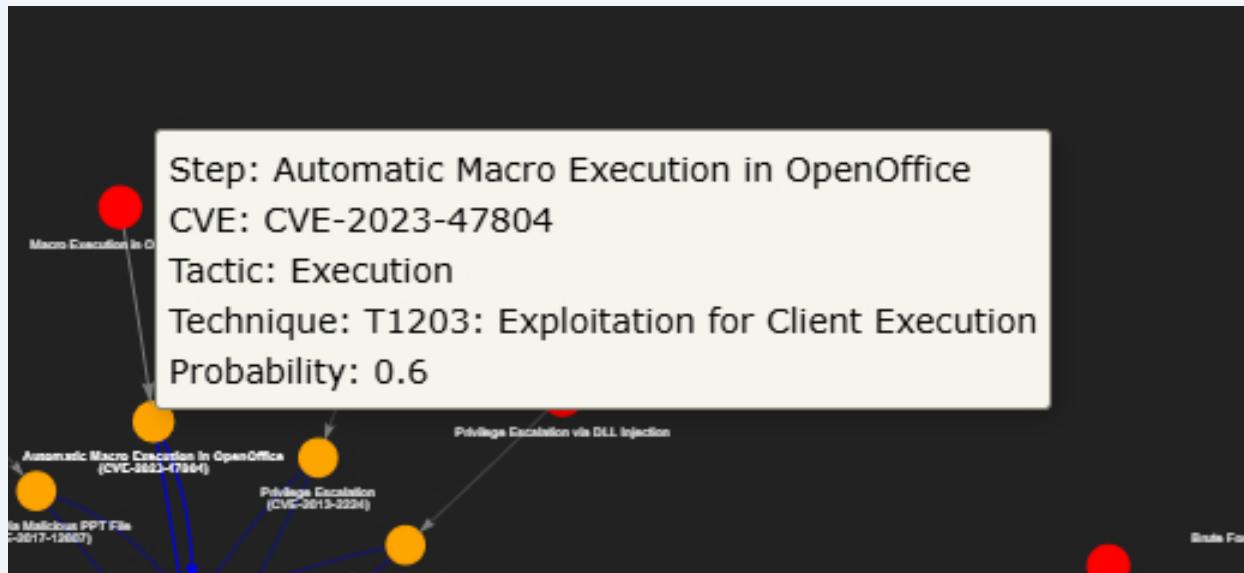
CVE ID	Nodes Affected	Impact Score	
CVE-2015-7833	22	107.8	<button>Patch</button>
CVE-2023-47804	9	79.2	<button>Patch</button>
CVE-2022-37401	9	79.2	<button>Patch</button>
CVE-2021-33035	9	70.2	<button>Patch</button>
CVE-2017-12607	9	70.2	<button>Patch</button>
CVE-2020-13958	9	70.2	<button>Patch</button>
CVE-2013-2224	10	69	<button>Patch</button>
CVE-2013-1935	10	57	<button>Patch</button>
CVE-2013-2188	10	47	<button>Patch</button>
CVE-2012-3440	7	39.2	<button>Patch</button>

65

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

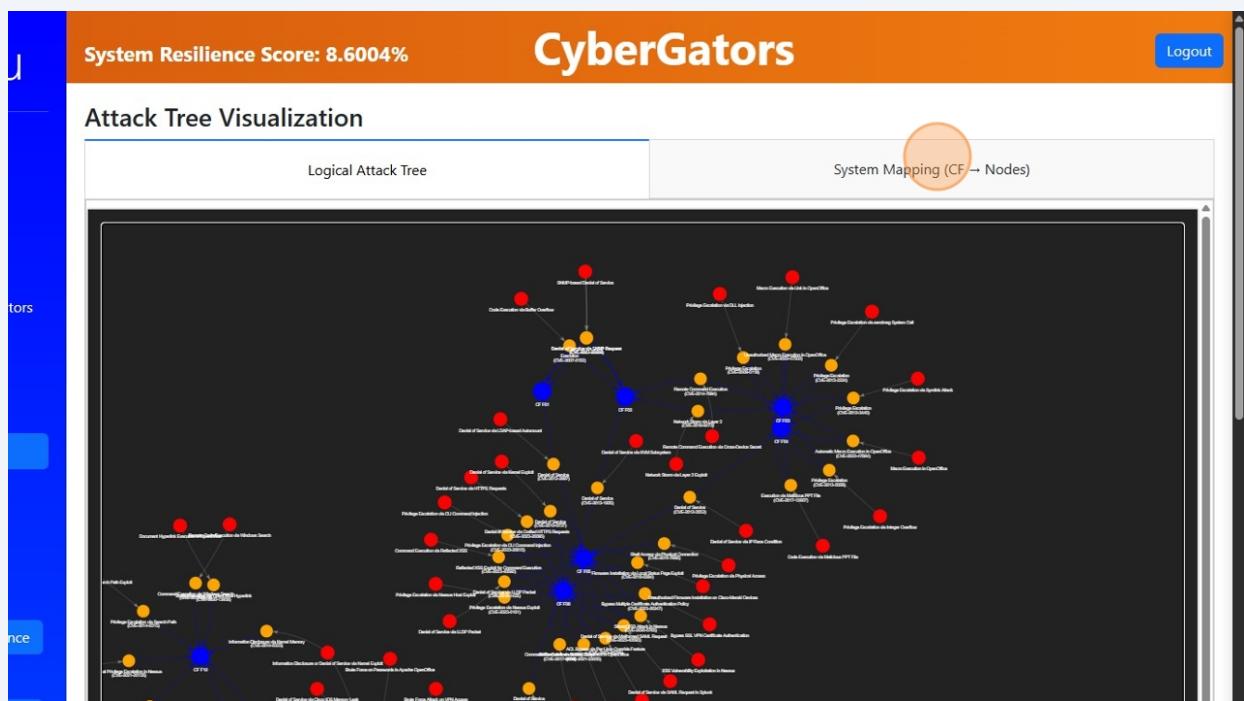
66

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

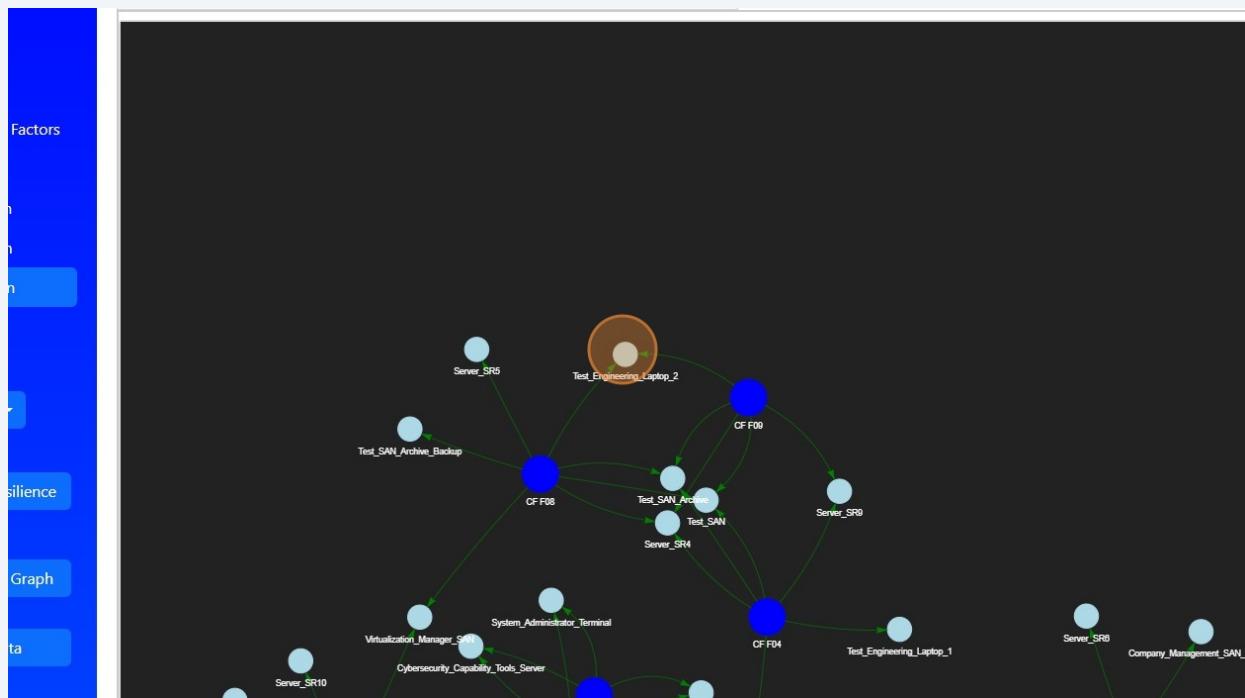


67

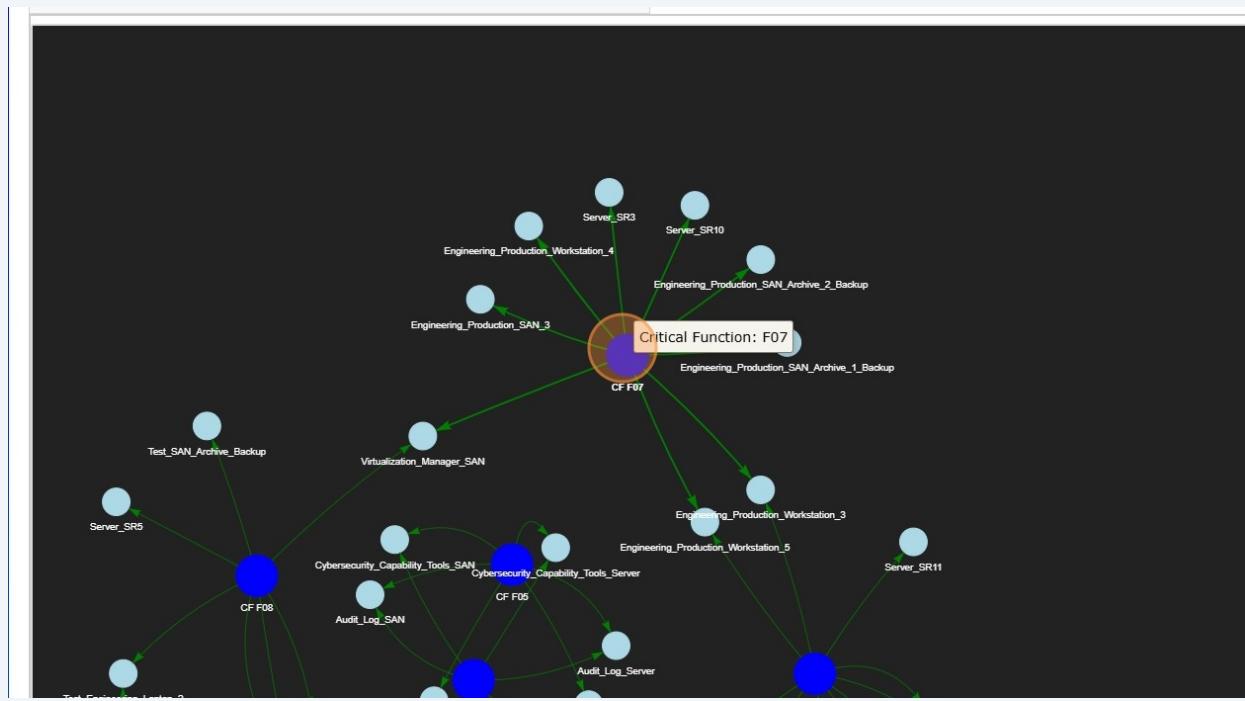
To view the association between the nodes and Critical Functions, click "System Mapping (CF → Nodes)"



68 To start the simulation, select the starting node.

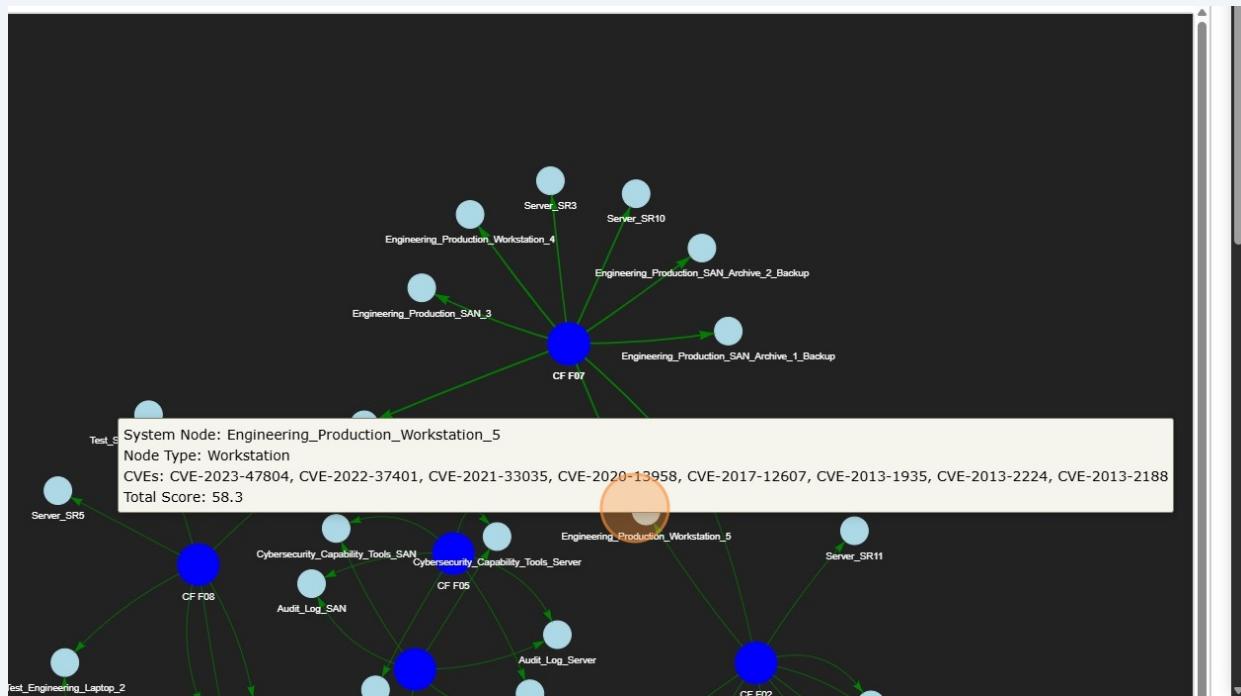


69 Select the traversal node



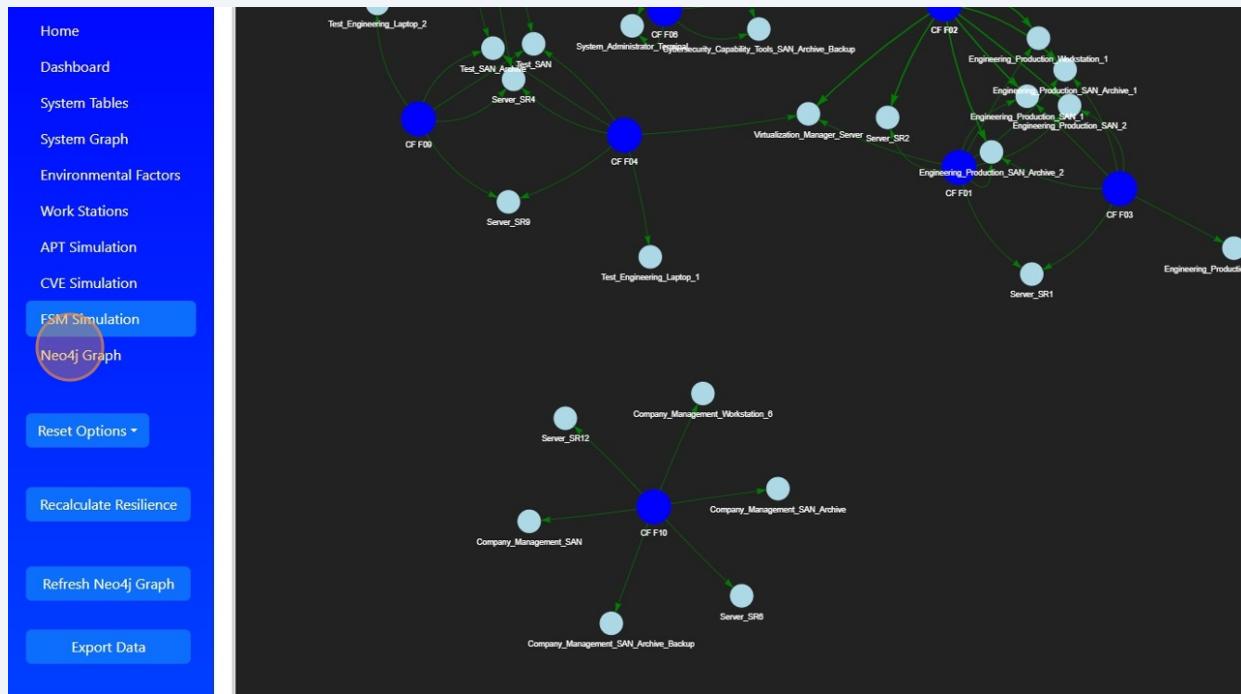
70

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.



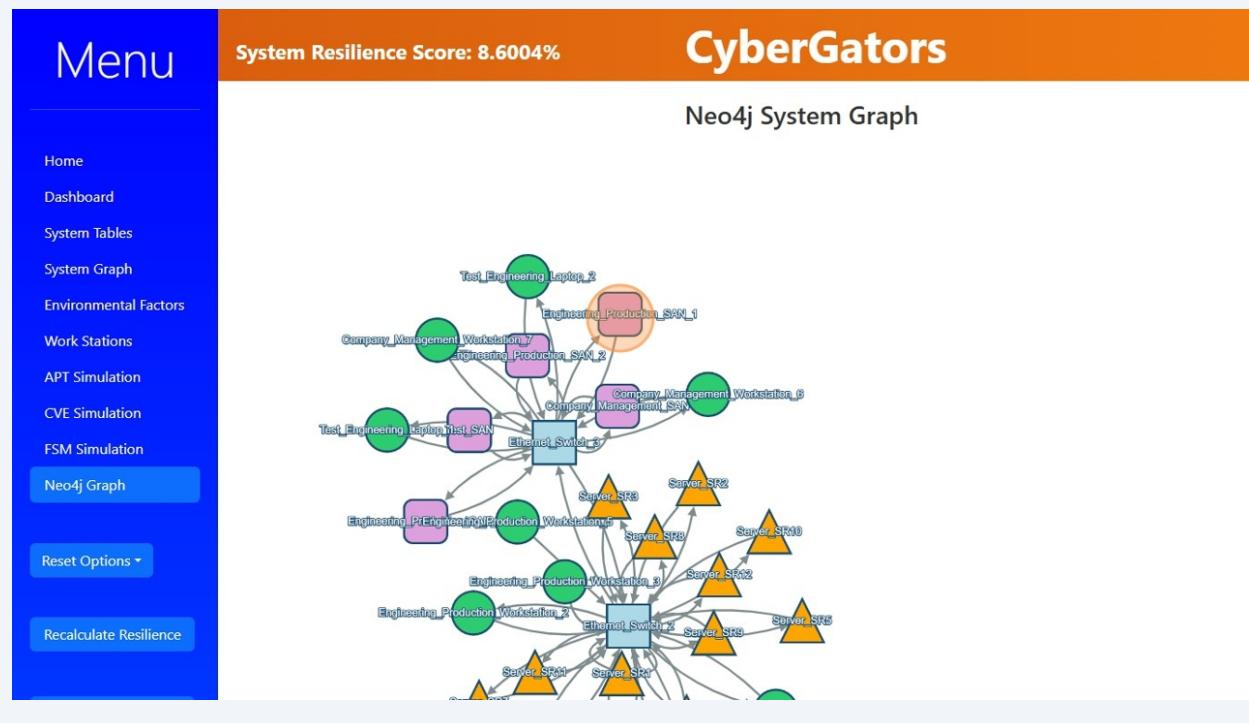
71

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



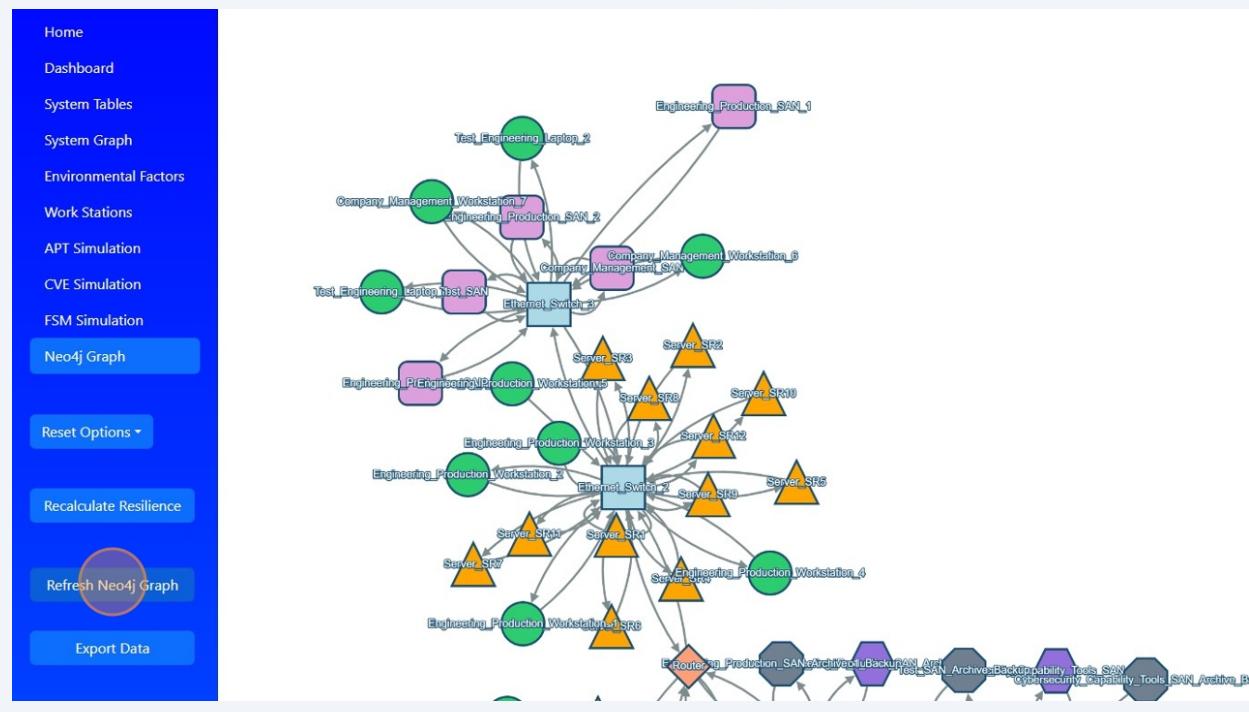
72

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"

The screenshot shows the Neo4j Graph interface. On the left, a sidebar menu lists various system management options: Home, Dashboard, System Tables, System Graph, Environmental Factors, Work Stations, APT Simulation, CVE Simulation, FSM Simulation, Neo4j Graph, Reset Options (highlighted with a red circle), Recalculate Resilience, Refresh Neo4j Graph, and Export Data. The main area displays a detailed network graph with nodes representing different system components like Workstations, Servers, Ethernet Switches, SANs, and Firewalls, connected by bidirectional arrows indicating their relationships.

75

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

This screenshot is similar to the previous one, showing the Neo4j Graph interface. The sidebar menu includes the same options, with 'Reset Options' highlighted by a red circle. A dropdown menu is open under 'Reset Options', showing the following items: Reset All (highlighted with a red circle), Reset Nodes, Reset Software Inventory, Reset Attack Tree, Reset Risk Factors, and Reset Work Areas. The main area shows the same network graph as the first screenshot.

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.

The screenshot shows a web application interface for CyberGators. At the top, there is a navigation bar with a user icon, the text "System Resilience Score: 8.8506%", the "CyberGators" logo, and a "Logout" button. Below the navigation bar, the main content area has a title "Export Data". A descriptive text states: "CyberGator allows users to generate detailed reports on their system's resilience assessments." followed by a bulleted list: "• Download reports in CSV or PDF format.", "• Share findings with security teams for further analysis.", and "• Maintain historical records to track improvements over time.". Another text block says: "These reports provide valuable documentation for cybersecurity planning and compliance audits." Below this, there is a section titled "Select which Data Table and Scores to export." with several checkboxes: "Nodes" (checked), "CVEs", "Software Nodes", "Critical Functions", and "Unique Software". At the bottom of this section is a large blue button labeled "Export Data to CSV".