ThreatModeler
SECURITY STARTS HERE

2020

ThreatModeler™: Interface Guide

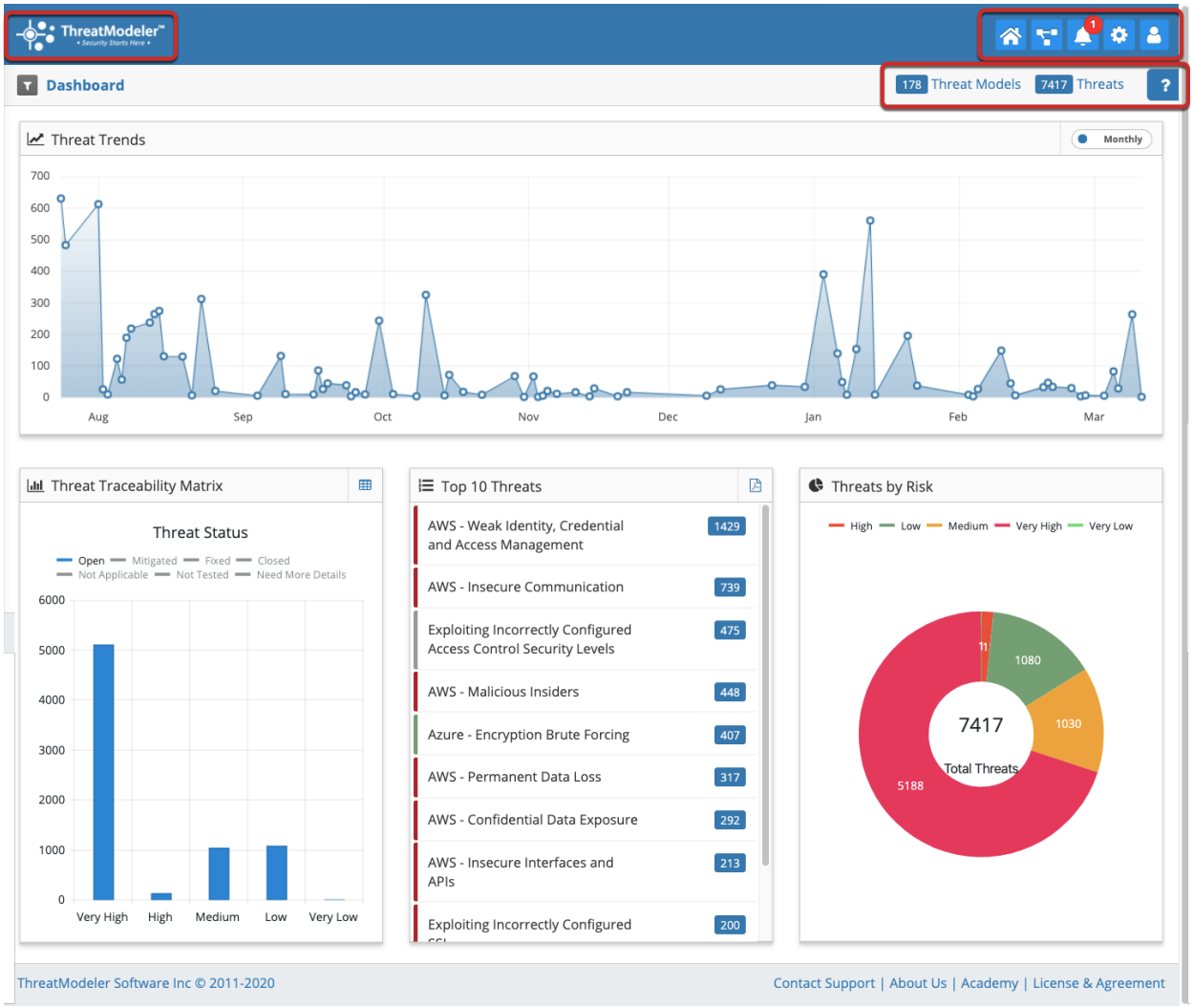
THREATMODELER SOFTWARE, INC. I 185 HUDSON STREET, SUITE 1620, JERSEY CITY, NJ 07311 I 201-266-0510

Table of Contents

Navigating the ThreatModeler™ Platform

Dashboard

After you login, you will be taken to the Dashboard landing page, which functions as the Home page.



Dashboard Contents

After authentication, you will be taken to the Dashboard, which contains an overview of all the threats across your IT environment based on threat models built. You can view the total number of threat models and threats presented in different formats.

Primary Navigation Bar

The static header has buttons on the left and right, enabling you to perform various functions.

Static Header Buttons

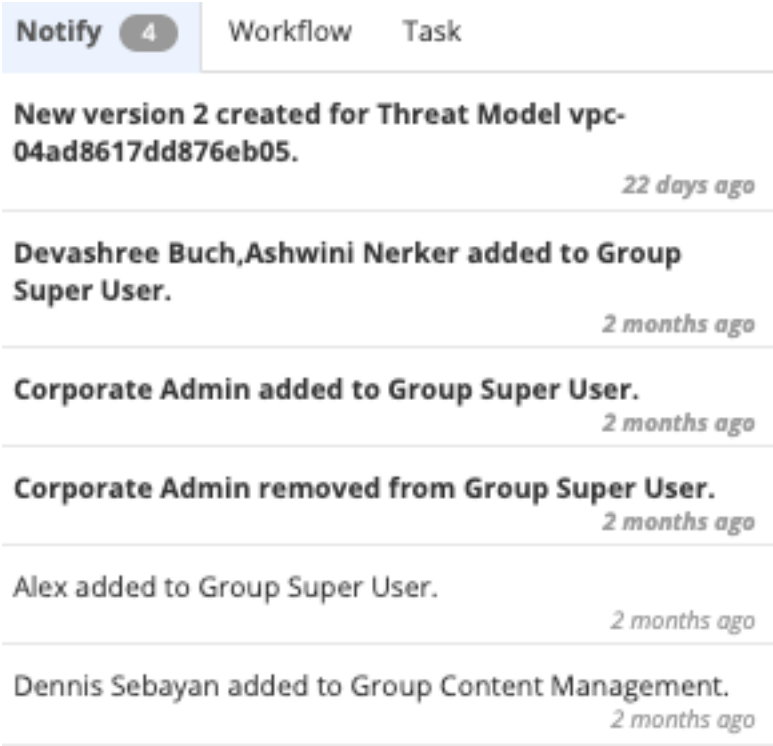
ThreatModeler Logo – located in the upper left-hand corner, click to bring you to the Dashboard from any screen.

Icons – use the top header buttons on the right to quickly navigate to ThreatModeler pages.


Home – Click to navigate to the Dashboard.


Threat Models – Click to go to the main list of threat models that are available to the user. The user's authorization level and Group inclusion – as designated by the platform administrator – determines how the list is populated.

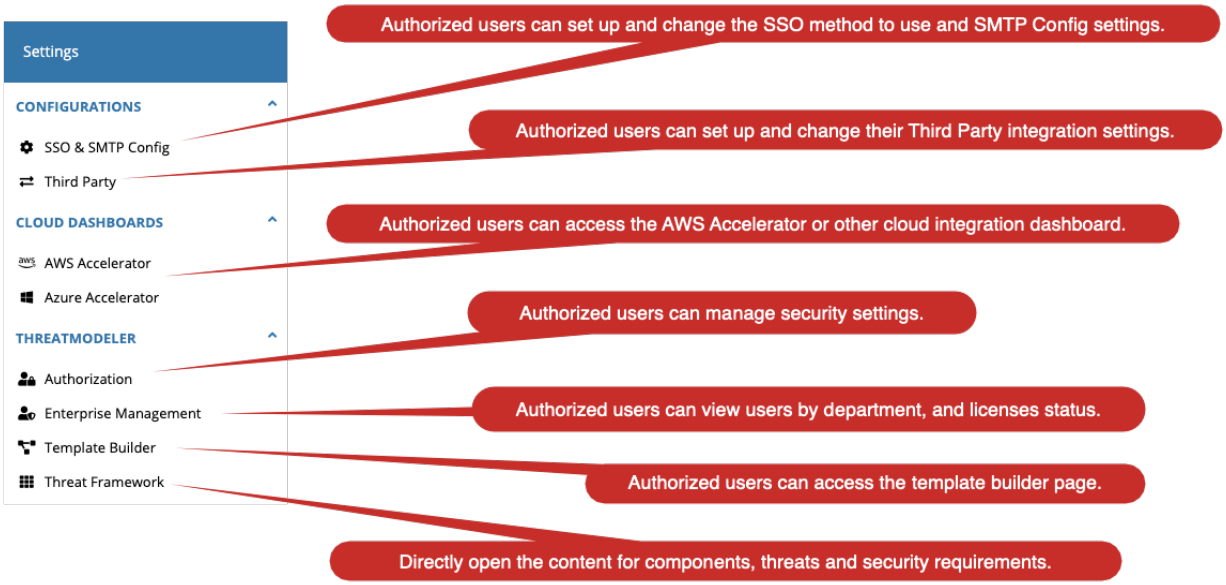

Notifications – Click to see a popup of information relevant to the user.




Settings – Click on the gear icon to view a slider menu, which enables the user to manage certain settings within the platform. Access to settings is based on the user's authorization level.

Settings Pull-Down Menu

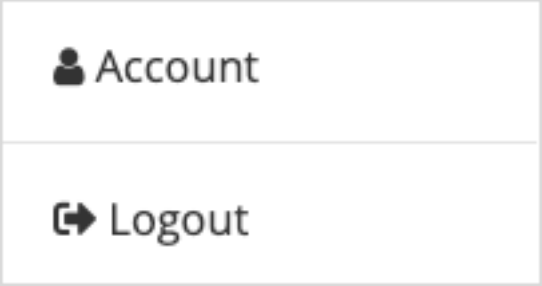
The Settings pull-down menu is organized with three main subheadings: Authorizations, Cloud Dashboards and settings specific to the ThreatModeler platform.



Account Profile

Click to view account profile information (including your account information, Name, Email, Department and Last Login).

1. You can also log out of ThreatModeler.
2. Logging out will return the user to the Authentication Screen.
3. Click on Account to manage your account profile options, including to reset your password.



Dashboard Menu

The Dashboard Menu enables you to deep dive into information summarized on the dashboard. Buttons for Threats and Threat Models Buttons are labeled with quantities for each. In the below screen shot, there is a total of 2,664 threats identified within the 103 threat models summarized.

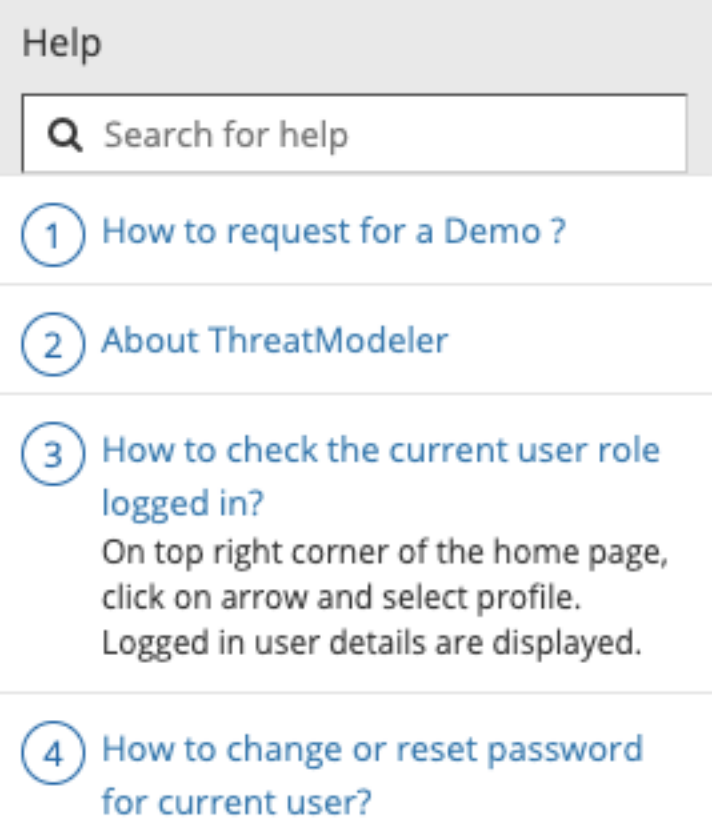
1. Click Threat Models to navigate to the primary Threat Model screen.
2. Click Threats to navigate to the Threat Portfolio screen.

Help Icon

On the far left of the Dashboard menu and accessible on every screen is the Help icon. The Help Icon contains frequently asked questions (FAQs) and a search bar.

Click on the  icon to open the Help Menu search bar and FAQ list.

- Input text in the search bar for the most relevant results.
- Click on questions on the list to expand on the answer.
- Click on the selected question again to close the answer, which closes the Help Menu.



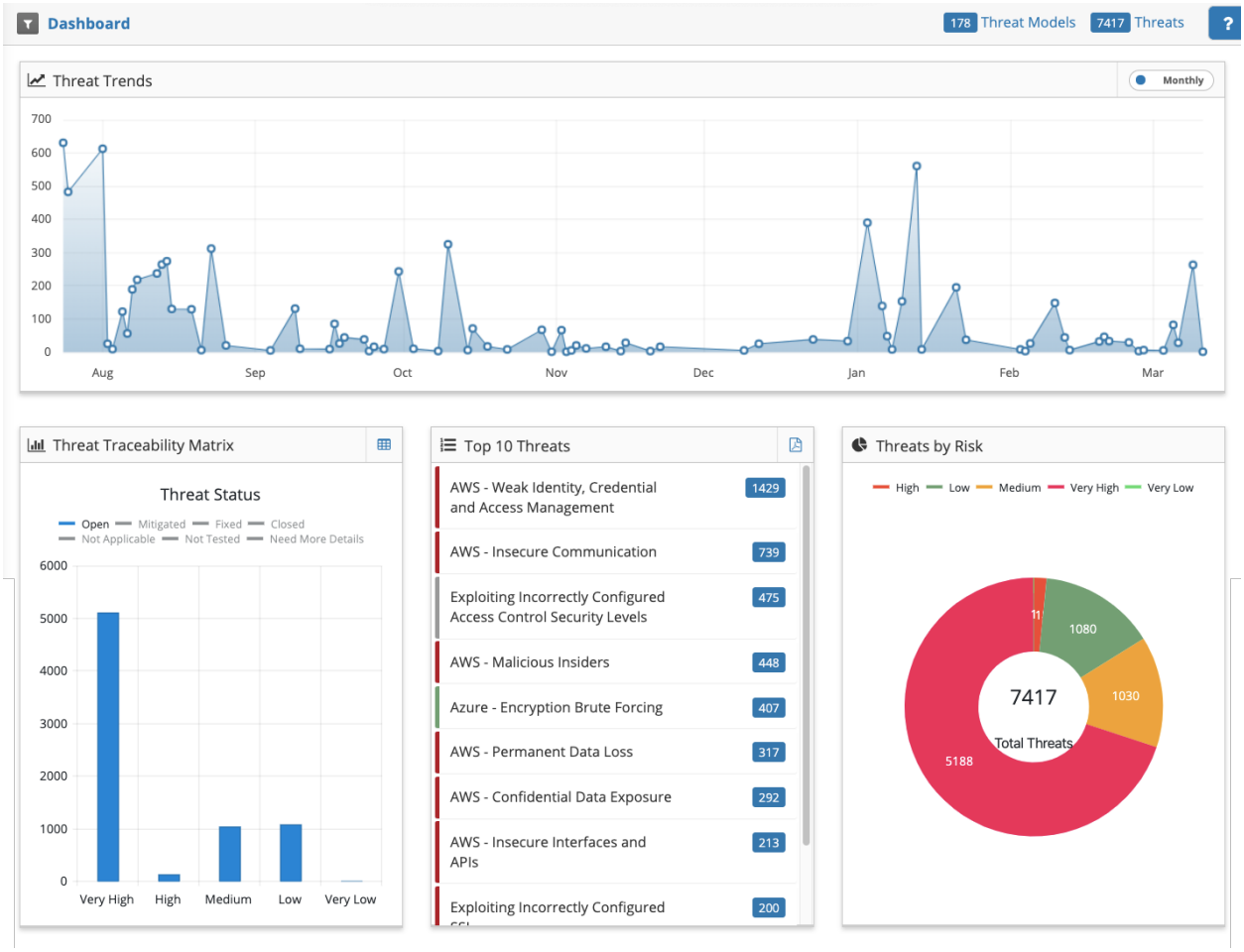
A static header exists on all ThreatModeler pages that provides you quick access to, among other displays, of:

- Threat models
- Templates
- Settings

View Threat Data in the ThreatModeler Dashboard

The dashboard is the default view when you log in to ThreatModeler. It displays threat data in different formats, that represent your Threat Risk Profile. Prioritize threats based on relevancy, including their:

- Trends
- Risk level
- Date threats were identified
- Status



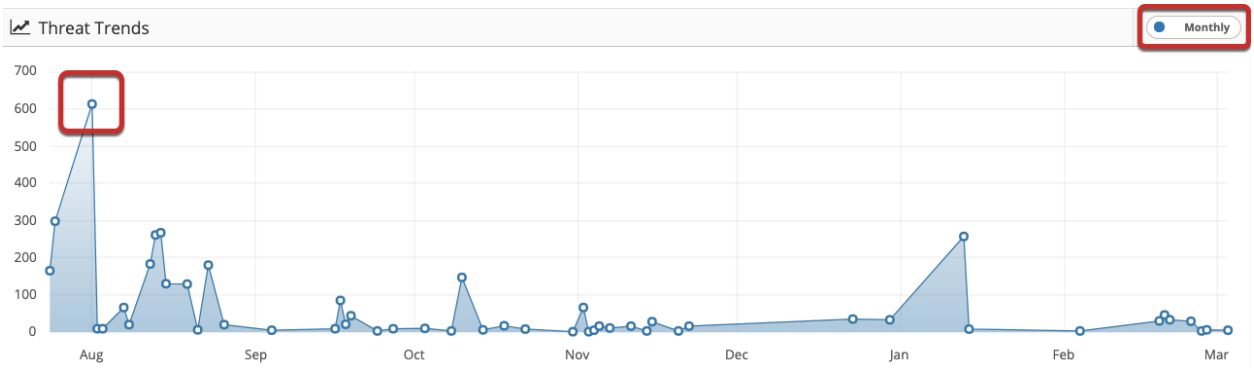
Four Main Panels in the Threats Dashboard Are All Interactive

Each panel in the Threats Dashboard contains information listed in various views so you can analyze threat data associated with your threat models.

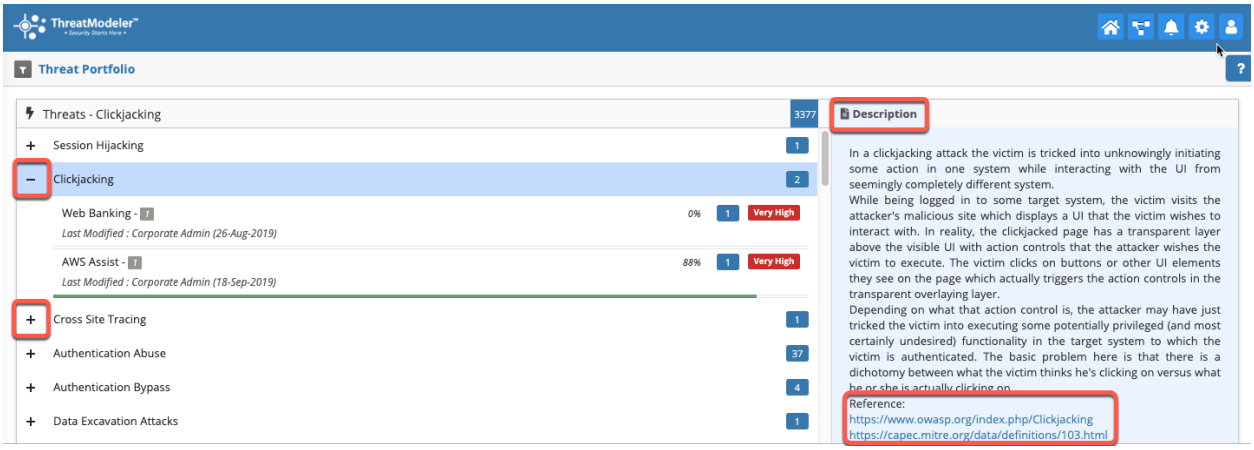
Threat Trends

The Threat Trends graph displays the number of threats that were added on a particular day.

1. Hover over a point on the graph to view the number of threats for that corresponding day.
2. Double click on a point in the graph to navigate to the Threat Portfolio, where you can see the threats for that corresponding day in a list.
3. Click on the icon in the upper right corner to display the graph either Monthly or Quarterly.



Threat Portfolio



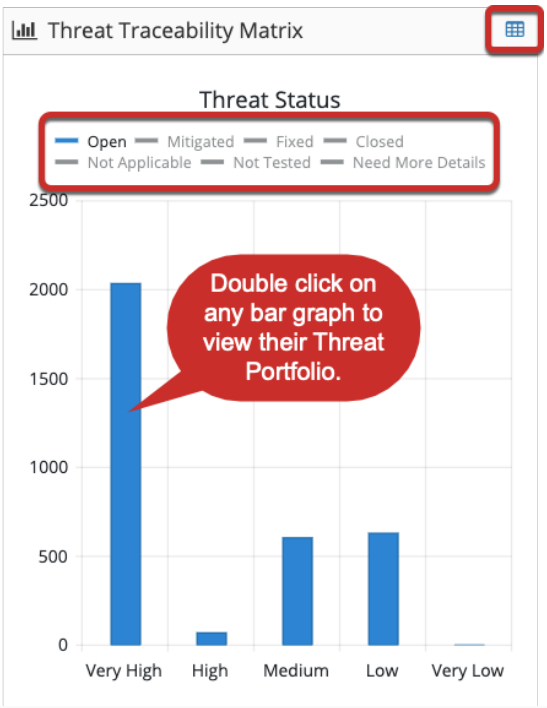
1. On the Threat Portfolio screen, click on the  icon to the left to view which threat model(s) are associated.
2. The Description field on the right contains content outlining the threat type and vulnerability that can increase risk. When applicable, the Description includes a reference link.
3. Click on the icon to close the expanded view.

You will also be able to view:

- The risk severity level that the threat poses to each model, which can range from Very Low, to Low, to Medium, to High to Very High.
- All the individual model information normally present on the Threat Model Summary Page.

Threat Traceability Matrix

The Threat Traceability Matrix gives you a quick understanding of the organization's threat by risk and status. The Threat Status groups the threats model by status. The default view is a bar graph. In the alternate table view, you can see all the threats listed by status.



Threat Traceability Matrix

Status	Very Hig	High	Medium	Low	Very Low
Closed	1	4	0	0	0
Fixed	1	0	0	0	0
Mitig...	39	0	1	0	0
Need More Deta...	0	0	0	0	0
Not Appli...	0	0	0	0	0
Not Tested	0	0	0	0	0
Open	2035	68	600	627	1

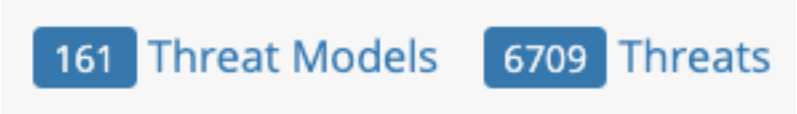
1. Change the chart from table to bar graph view by clicking the toggle button in the top right-hand corner.
2. Select and deselect the threat status type you want to view in the graph (Open, Mitigated, Fixed, Closed, Not Applicable, Not Tested, Need More Details) by clicking on the line buttons above the graph.

3. Hover over a bar on the graph to view a count of each component.
4. Double click on the graph bars to navigate to the Threat Portfolio page.
5. Toggle between graph and table views by clicking on the icon on the top right.

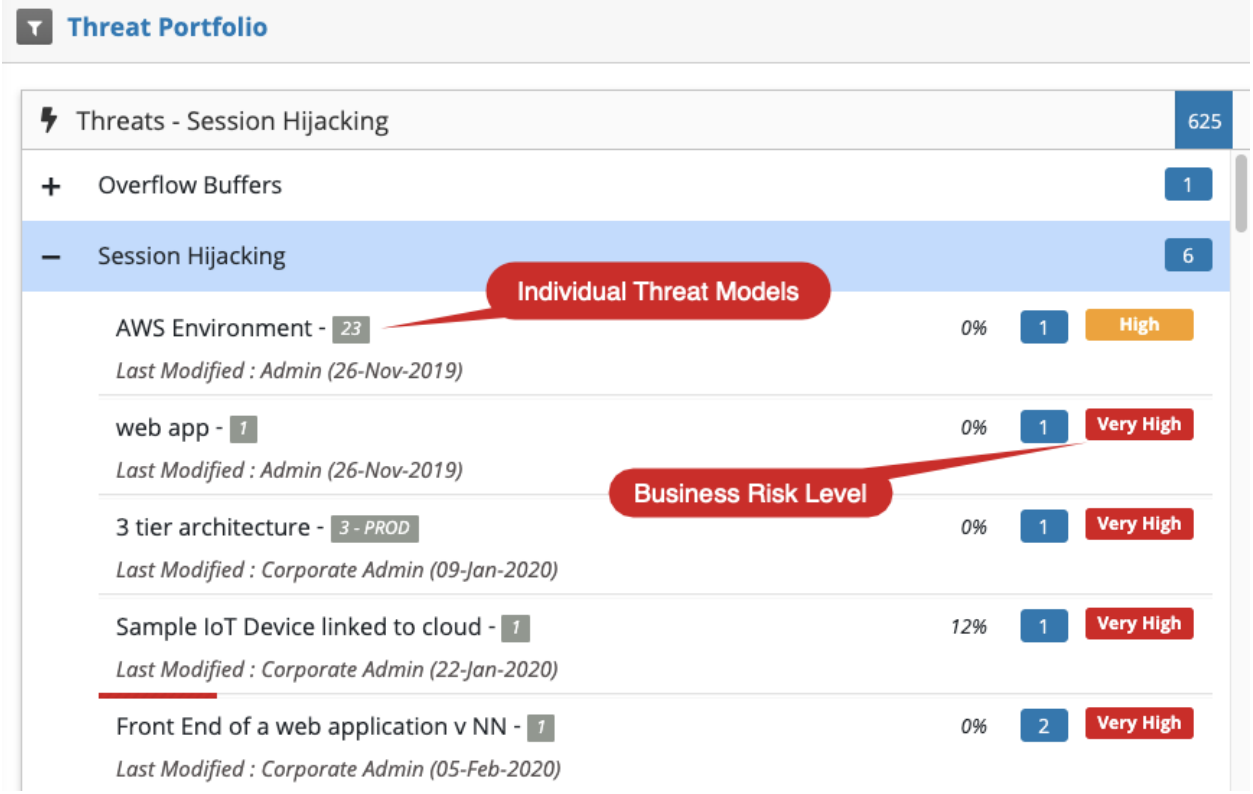
Reminder: If you need to navigate back to the main Dashboard from any screen, you can always click on the ThreatModeler logo on the top left of the static header. You can also click on the Home  icon on the top right of the static header.

Threat Counter

The counters show how many times across all your models that a threat you highlighted was identified.



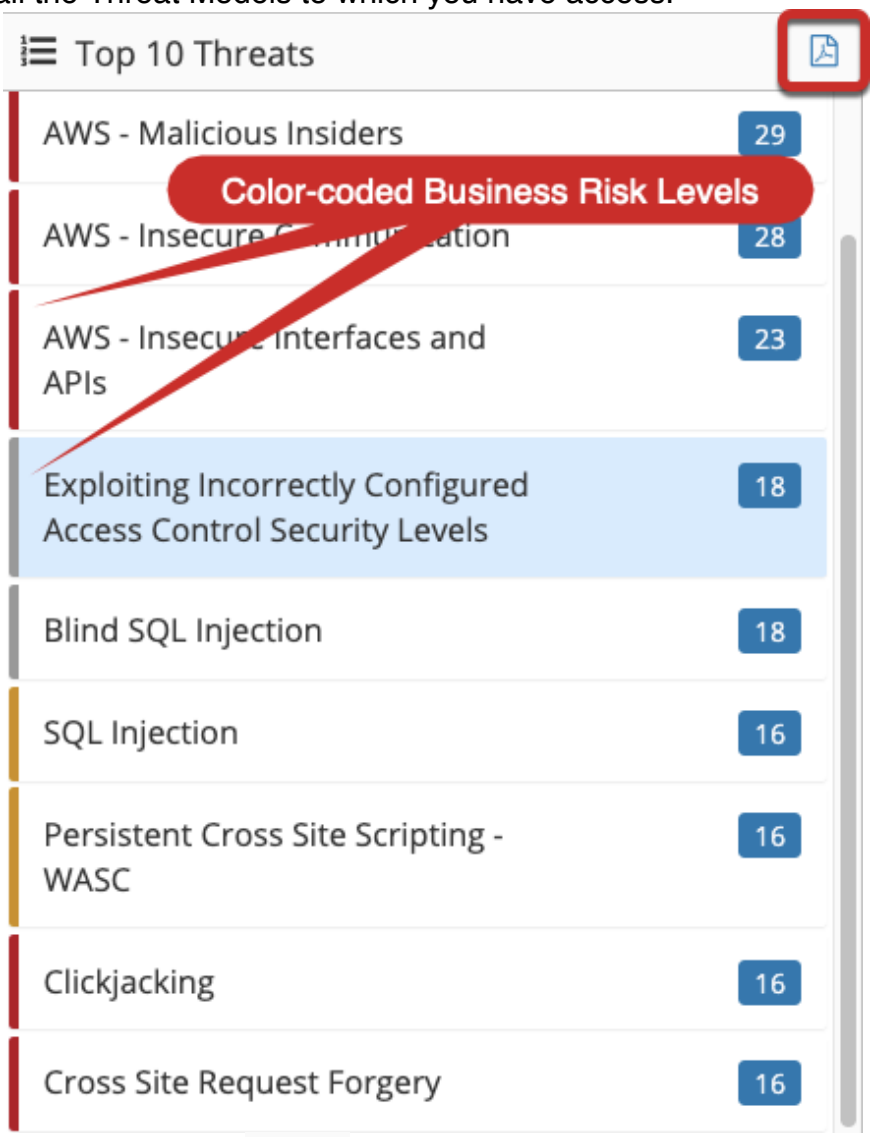
4. Click on Threats and you will be redirected to the Threat Portfolio screen.



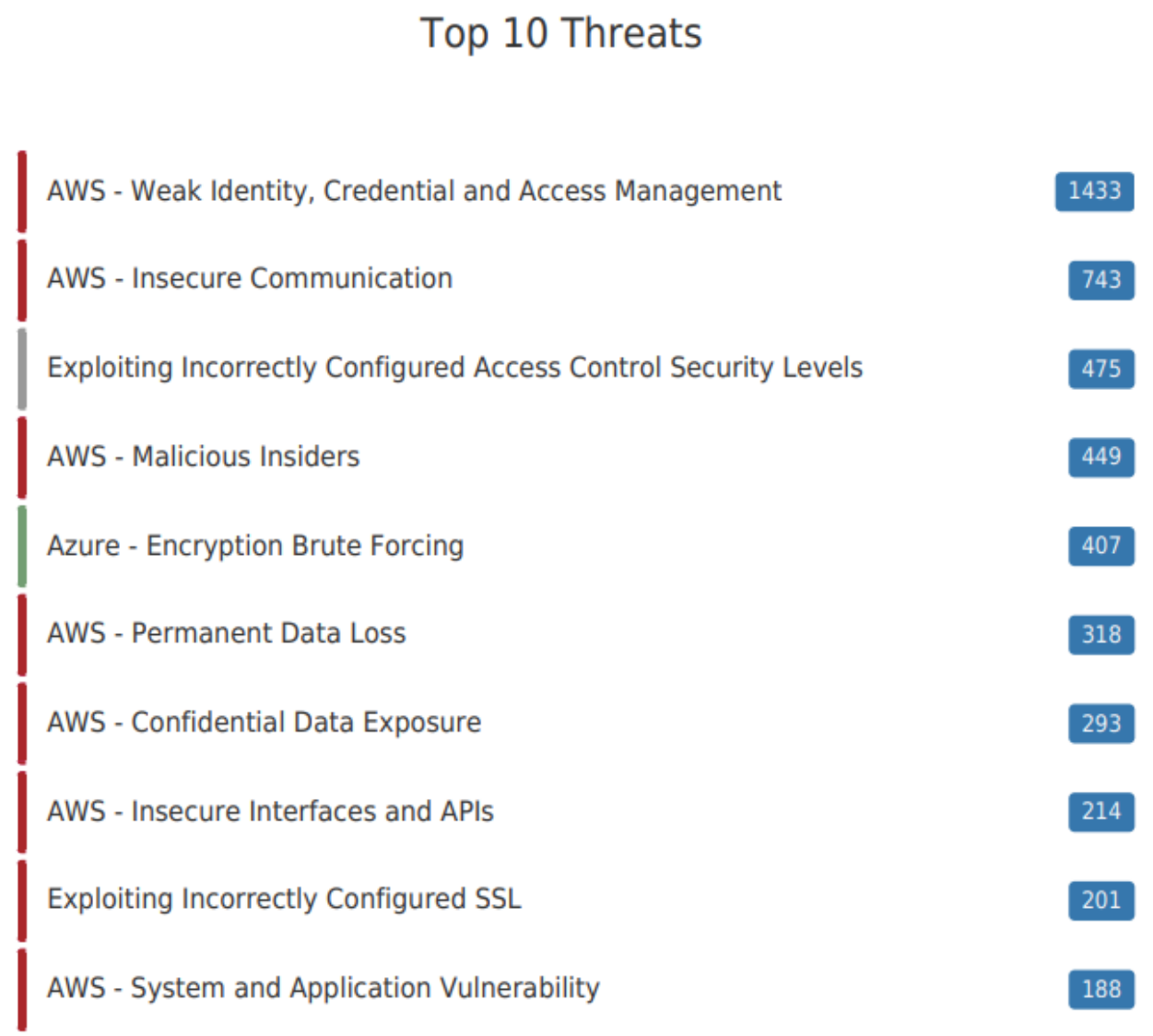
Top 10 Threats Widget

The interactive Top 10 Threats panel (located at the bottom center of the Home screen) allows you to click on a threat to display the impacted models in a list.

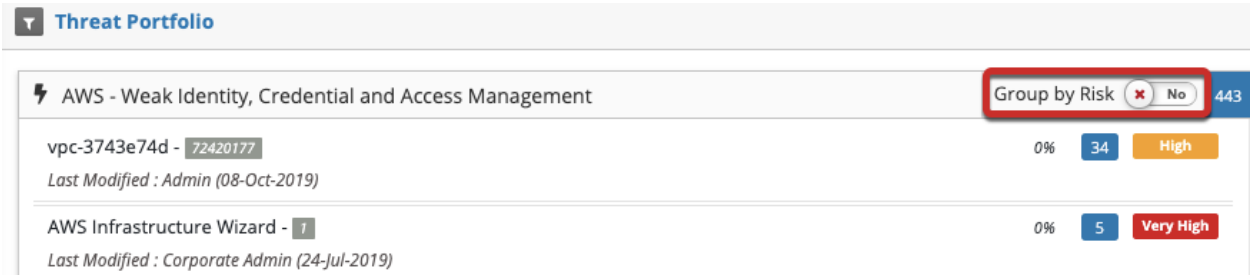
1. View an enumeration of the Top 10 Threats (most frequently identified threats) across all the Threat Models to which you have access.



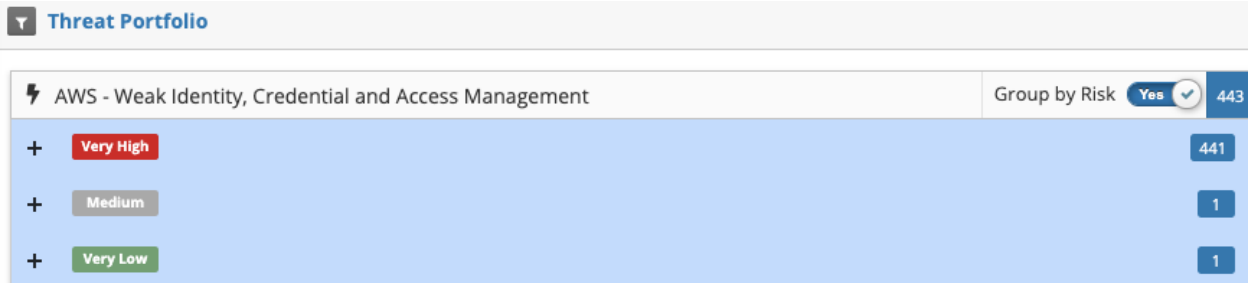
2. Export to a pdf using the  icon on the top right to communicate output to stakeholders. The PDF contains a:
    - List of the Top 10 Threats in descending order with the frequency tallied to the right.
    - Threat severity level indicator, color coded, to the left.



3. Double click on a point in the graph to navigate to the Threat Portfolio, where you can filter and deep dive into a particular threat, with a:
    - Threat description
    - List of threat models where the threat was identified.



Click on the Yes/No Group by Risk button and toggle to Yes to view an enumerated list categorized by risk level.

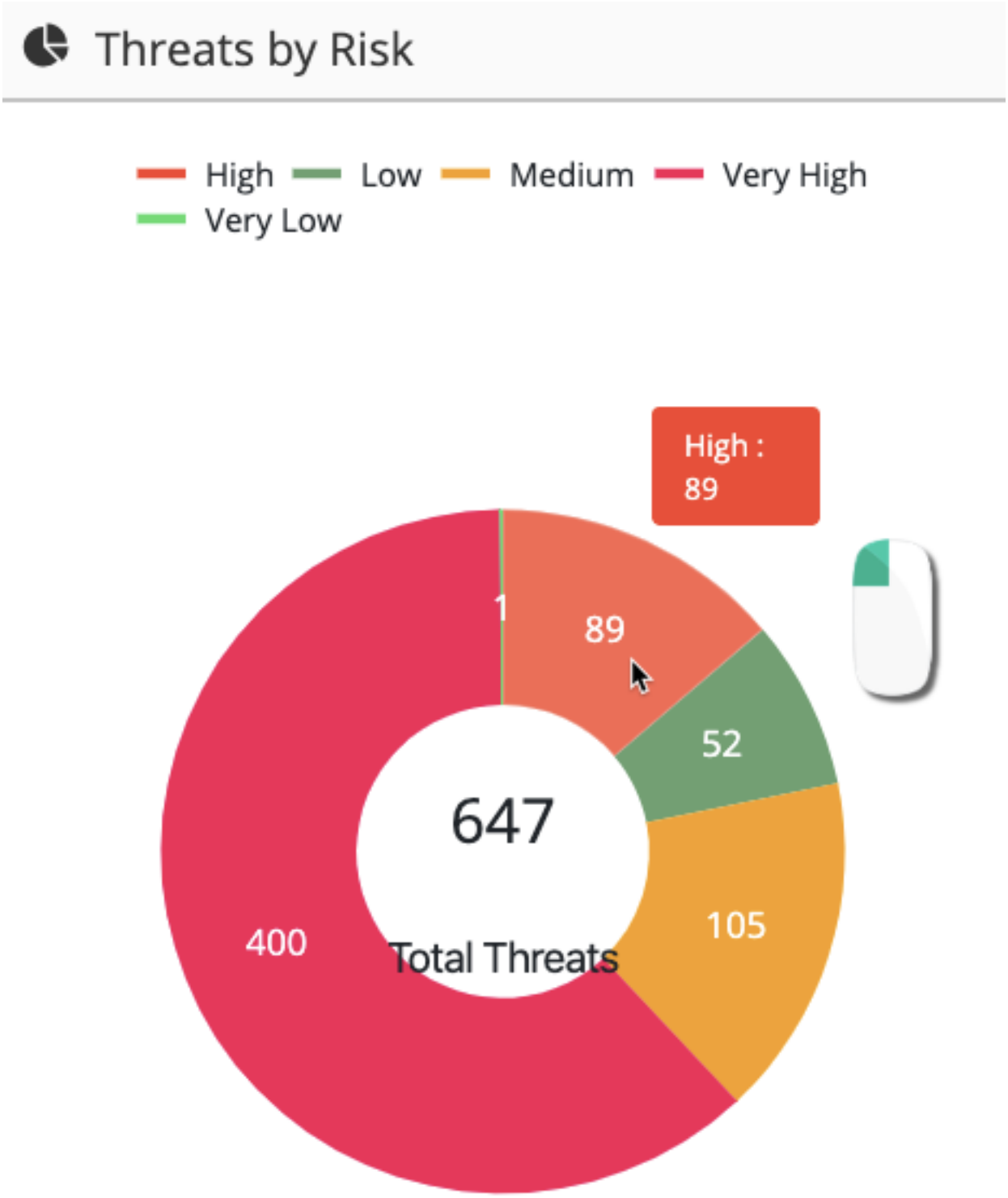


Threats by Risk

The Threats by Risk display, located in the lower right of the screen, shows a quick summary of threats in a pie chart (with counter) of all your threats, grouped by color according to risk severity level.

Hover your pointer over a section in the graph to see the level of risk that section represents.

1. Select or deselect the line buttons next to the risk level at the top to include or exclude different threat Groups on the graph (e.g., show only high or very high-risk threats).
2. Double click on a chart section to navigate to the Threat Portfolio, where you can deep dive into a list of threats associated with a certain risk level.

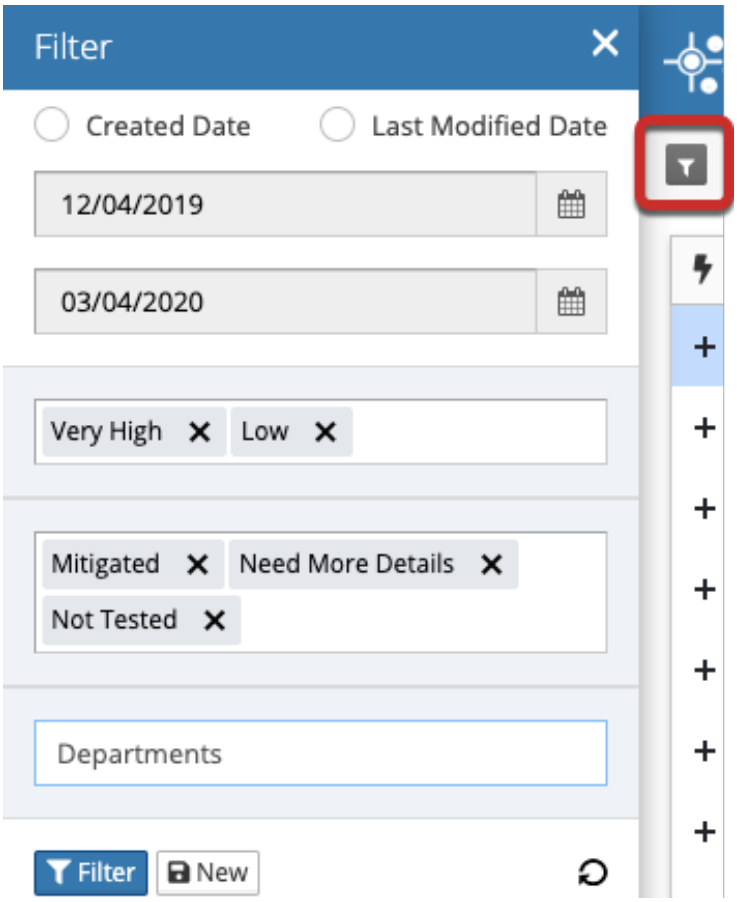


1. Once on the Threat Portfolio screen, click on the + icon to expand on a threat and view the threat model(s) where it was identified.
    - The counter at the top right shows the total number of times threats in that Group were identified.

- The individual threat counters show how many times the individual threat was identified.

Dashboard Filter

The Dashboard Filter is a sliding panel accessible on the far-left side of every screen. The contextual Filter changes all four panels when you input certain commands. Adjust your view based on the following options:

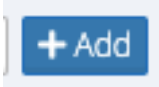


Dashboard Filter Elements

- Created Date vs. Last Modified Date
- Date Range with calendar widget
- Risks – from Very Low to Very High
- Status – Opened, Closed, Mitigated, Fixed, Not Applicable, Need More Details and Not Tested
- Department – Each user is assigned to a Department, which is created and edited in the Enterprise Management screen.

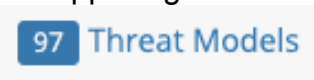
Saving a Filter for Repeat Use

1. Click on the 

button
2. Input a filter name and click 

button. You can also Cancel the procedure.
3. To **EDIT** the filter, delete it and create a new one.
4. You can also reset the filter by selecting 

Threat Models Primary Summary Screen

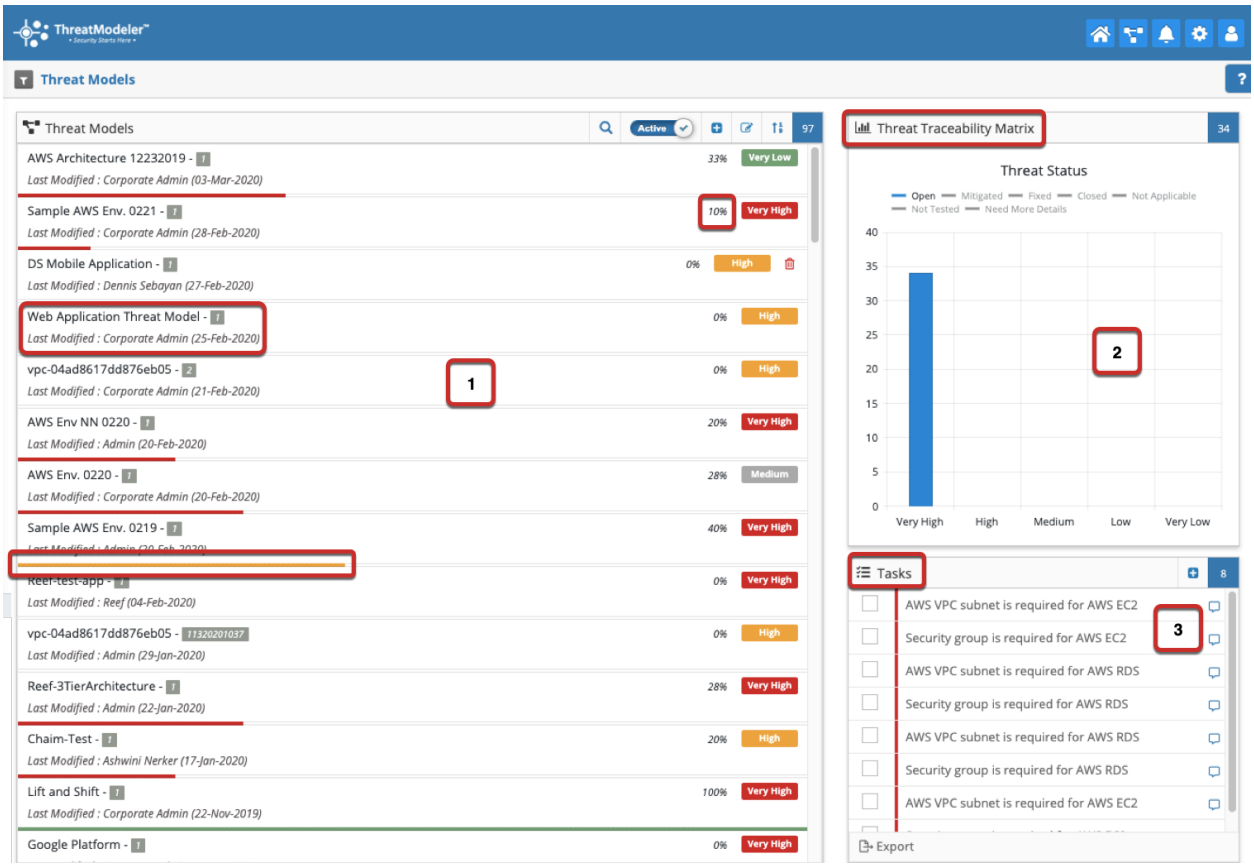
Access the Threat Models Primary Summary Screen by clicking on the  icon in the upper-right hand corner. You can also click on the Dashboard 

button

The Threat Models screen contains details for all the threat models the user can access (numbers correspond to the screen shot below):

1. Threat Models List
2. Threat Traceability Matrix specific to a particular threat model
3. Tasks Panel

Click on the corresponding Threat Models on the left to view the status of their threats.



On the tasks panel, you can also access the:

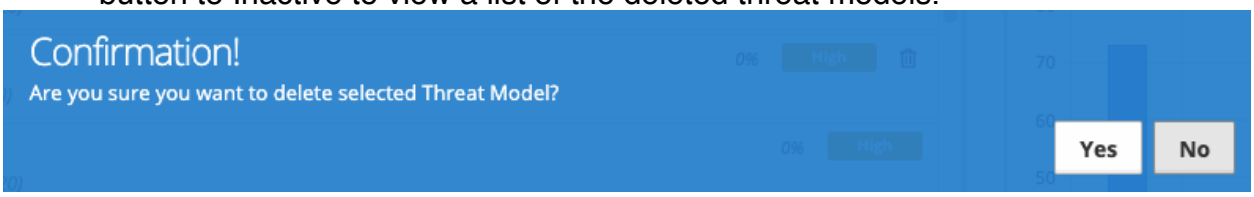
- Help function by clicking the  icon

- Filter Sliders – filter the threat models (e.g., by date and more) that are displayed in the three panels.

Threat Models List

The Threat Models List shows all the threat models that you are authorized to view. Threat models are listed by name and version in grey. Double click on a listed threat model to load a threat model in the Diagram screen. The Threat Models List also includes:

- Date it was last modified and by who (username)
- Percentage of task completion associated with a particular threat model
- Colored bar indicating completion status:
  - No bar indicates no tasks have been completed
  - Red bar indicates that most tasks are still open
  - Green bar indicates most tasks are completed.
- Risk status
- Any third-party integration
- Ability to delete the Threat Model by clicking on the icon, prompted with a final confirmation before deleting it. Once deleted you can Toggle the Active button to Inactive to view a list of the deleted threat models.

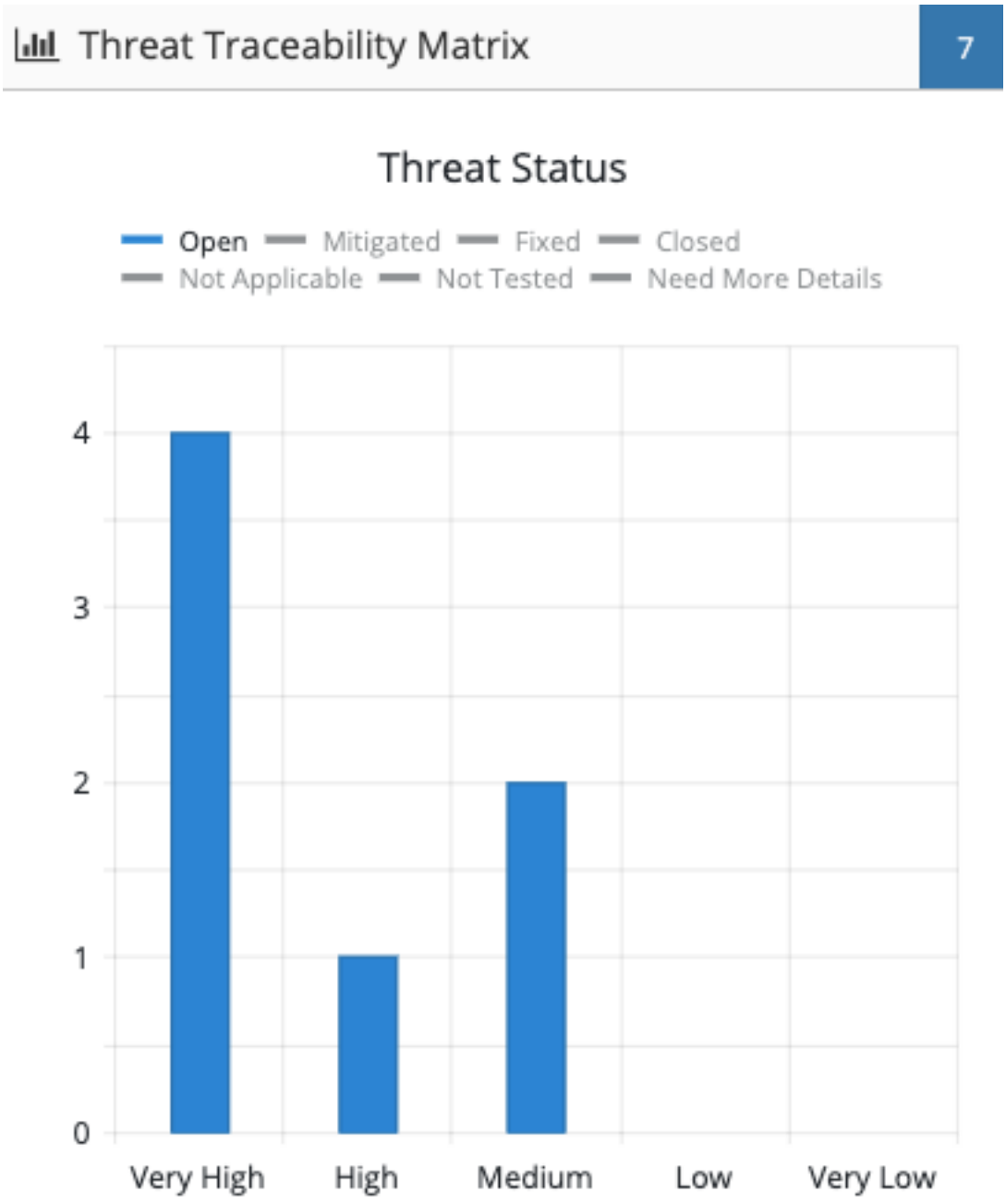


Threat Model Display Controls

The threat model display has controls that help you to manipulate the displayed list:

Threat Status Traceability Matrix on the Threat Models Primary Screen

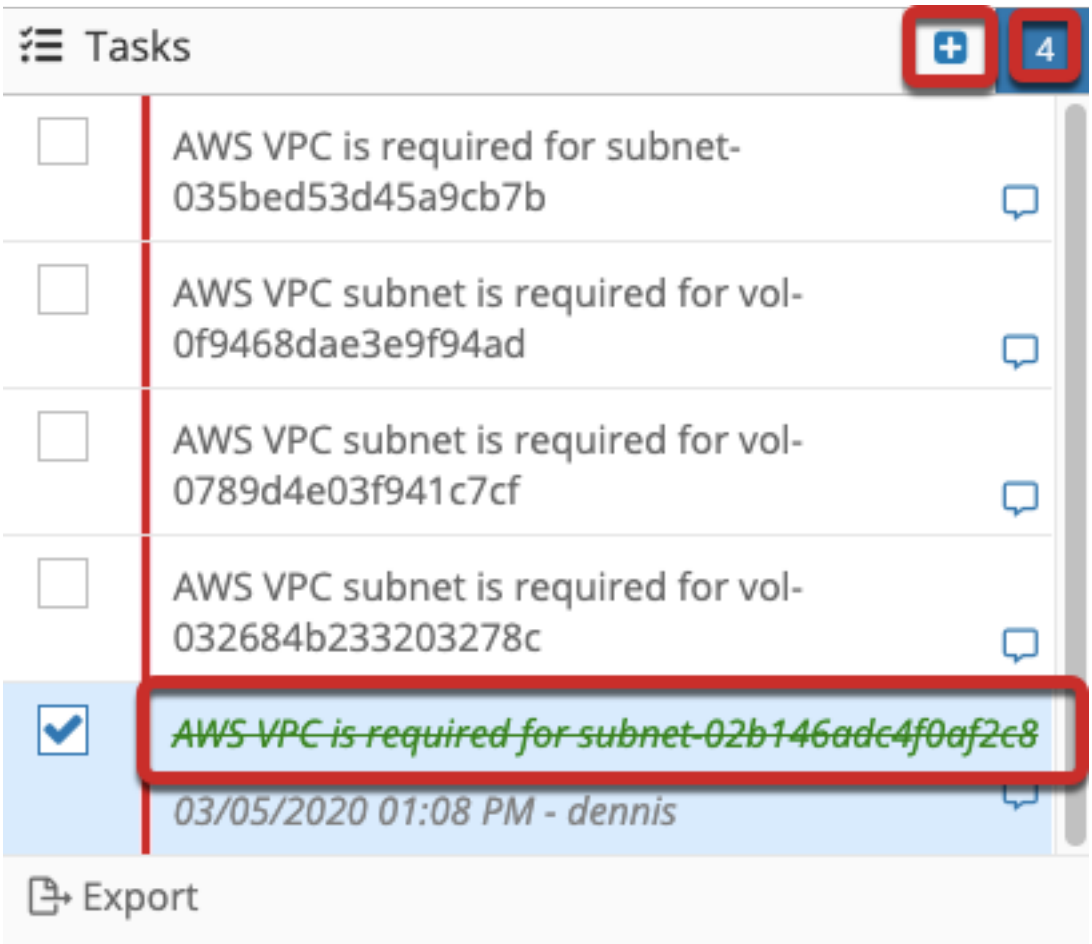
The Threat Traceability Matrix Widget on the Threat Model Summary Screen is very similar to the Threat Traceability Matrix shown on the Dashboard. It shows the number of threats, grouped by risk level and status. The counter in the top right-hand corner shows how many threats are included in the graph. Select or deselect statuses by clicking on the line buttons next to each status at the top. There is currently no way to toggle between displays as on the Dashboard Threat Traceability Matrix .



Tasks Panel

The Tasks Panel lists tasks associated with a threat model selected in the Threat Model List. Collaborators can add descriptions and notes to keep track of the conversation.

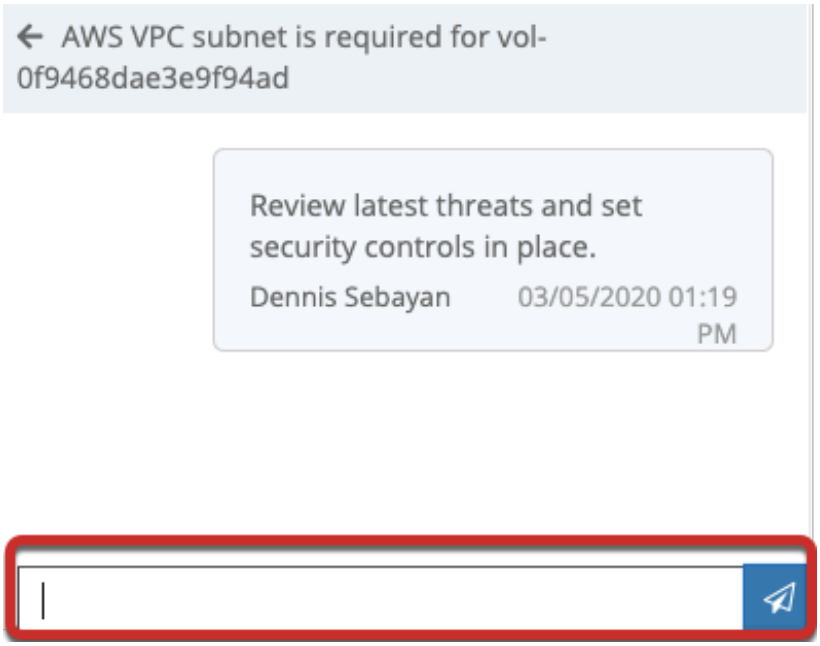
1. Add tasks by clicking the  icon.
2. Set a title for the task in the Define Task field and set the priority as High, Medium or Low.
3. Add an explanation in the free text Explain Task field.
4. Review the counter in the top right corner for the number of tasks waiting to be completed.
5. When a task is complete, check the box to cross it off. It will remain on the Task List, but the counter and percentage bar in the Threat Model List will be crossed out and highlighted in green.



Tasks Panel Collaboration

Users can add comments to a task by clicking on the  icon.

1. Type free text into the field at the bottom.
2. Click the send button. The comment will appear in the expanded view of the task, along with other collaborator notes.
3. Click on the  arrow to return to the Task List.
4. The  icon will now be blue to notify users that a comment was added.



ThreatModeler Diagram Screen

Threat models are created visually in ThreatModeler Diagram screen. As always, the Primary Navigation bar is located at the top of the screen.

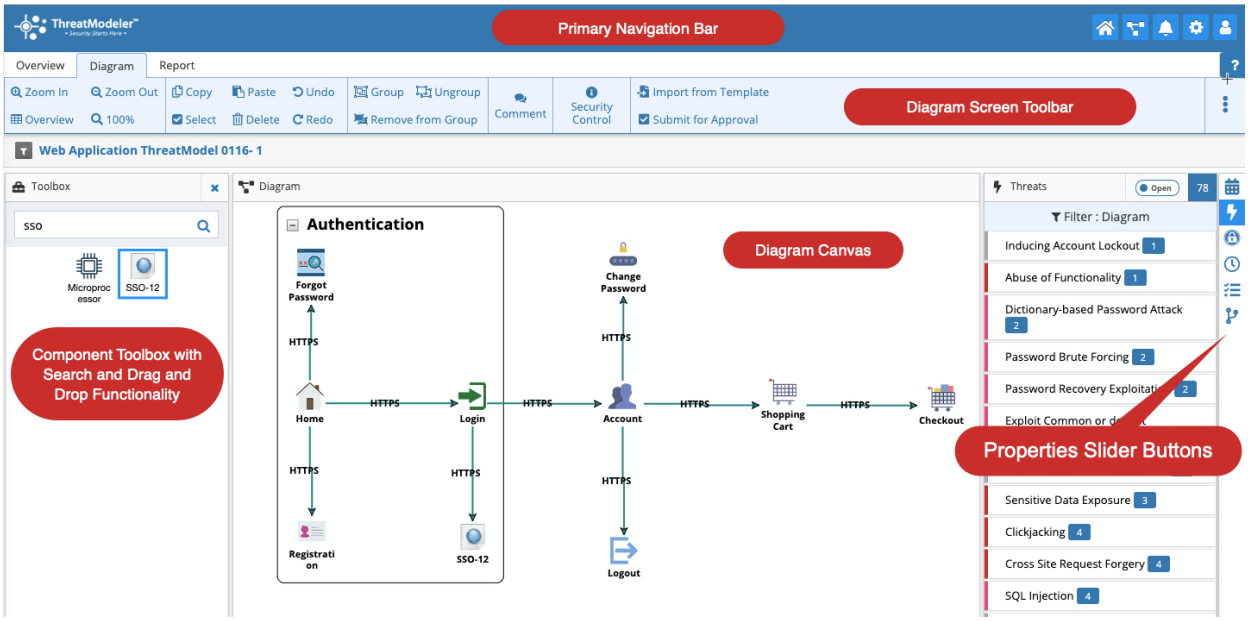


Diagram Toolbar

Users will find the Diagram Toolbar helpful for constructing threat models.

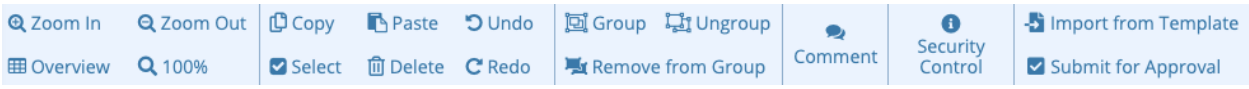
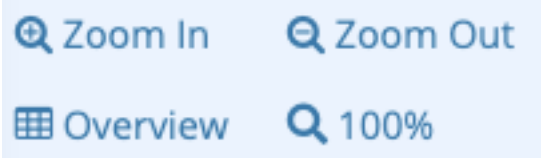


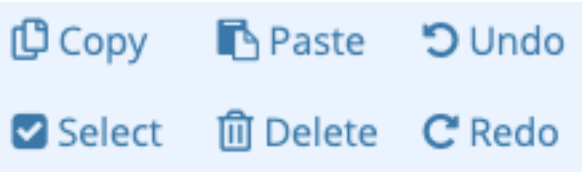
Diagram View Controls



The first set of toolbar controls enable you to manipulate the page view.

- Zoom In – increases the magnification of the Diagram canvas.
- Zoom Out – decreases the magnification of the Diagram canvas.
- 100% – adjusts the diagram size to display the entire diagram.
- Overview – places a small window in the upper left corner of the canvas that displays where the visible portion of the diagram resides in the full threat model.

Diagram Editing Controls



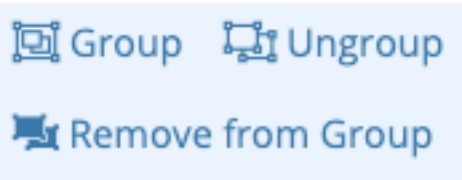
The second set of controls provides standard diagram editing functions including:

- Copy – copies any selected diagram items to the clipboard.
- Paste – places a copy of the clipboard item(s) on the canvas.
- Delete – removes selected items from the canvas.
- Undo – reverses the last diagramming action performed by the user.
- Redo – reverts back to the last diagramming action performed by the user.
- Select – highlights the entire diagram for editing.

Diagram Grouping Controls

- With Grouping, you can Group components and control them at once. Groups may be minimized by clicking on ⊟ to hide their contents, making the threat model diagram cleaner and easier to view. Once minimized, click on the ⊞ button to expand the Group view.

- Group — assemble and place selected components in a Group.
- Ungroup – separate the selected components, leaving the Group items unchanged.
- Remove from Group – releases the selected diagram elements from the next inner-most Group.



Comments

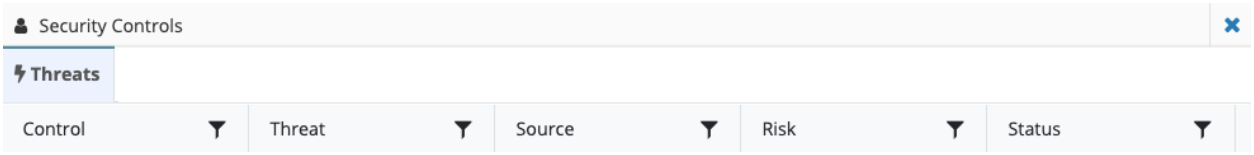
You can include comment free text within the diagram. Comments do not affect the way ThreatModeler analyzes the diagram. Once you've input the Comment, you can drag and drop it wherever you want in the Diagram.

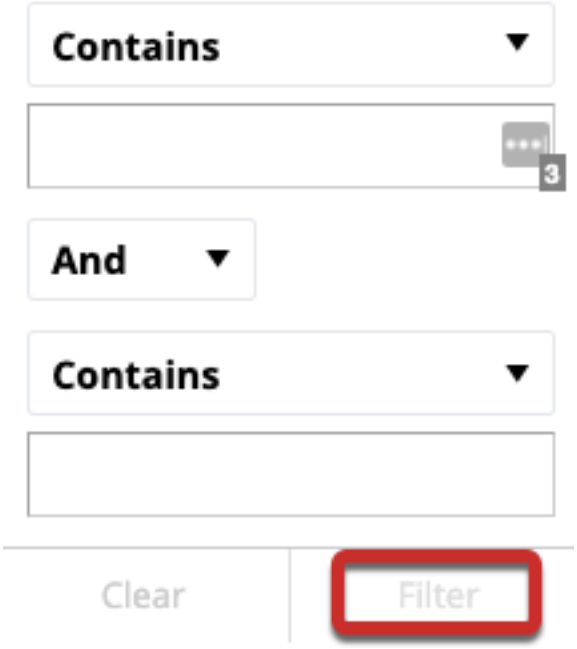
Security Control

The Security Control button enables you to view an enumerated list of security controls included in the threat model. Each column is filterable by keyword. Security Control Information includes:

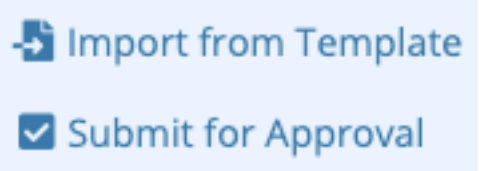
- Components associated with those threats
- Risk severity of threats
- Security controls used to mitigate the threats
- Threat status

1. Click the filter icon at the top of a column to filter that column.
2. Choose what you would like to filter by, then click Filter.
3. You can filter by multiple columns simultaneously.



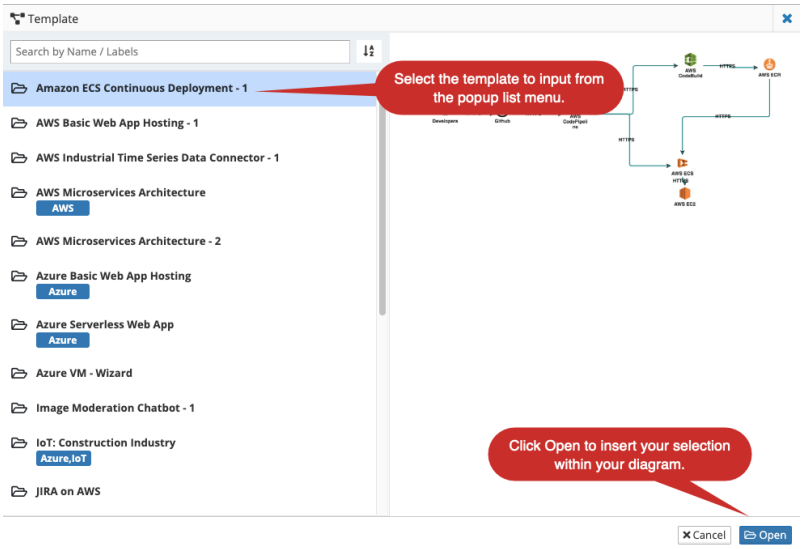


Import from Template Submit for Approval

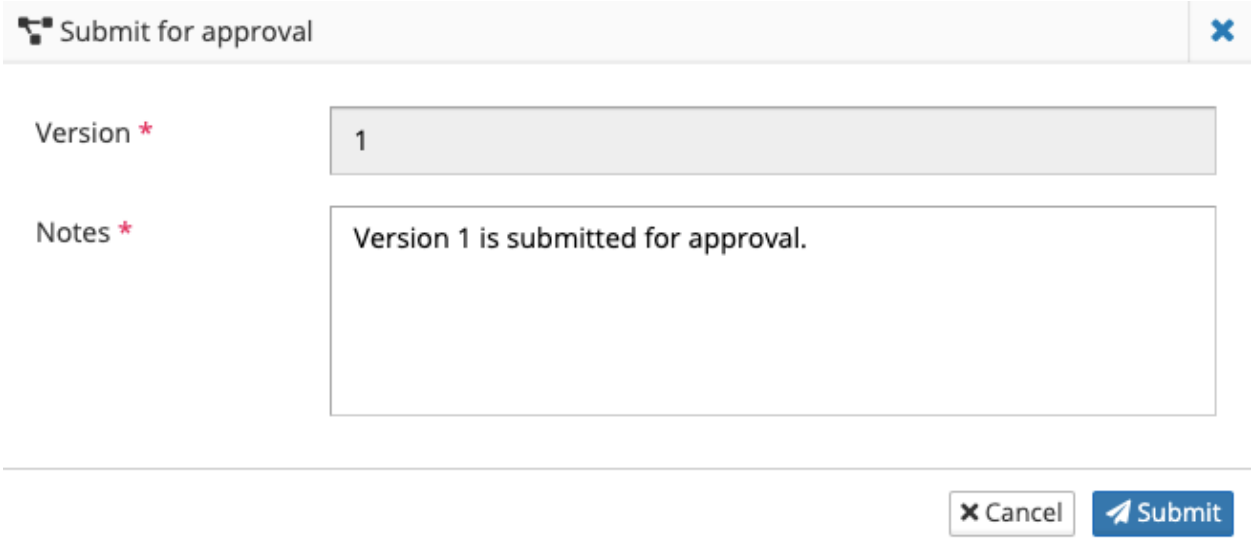


The last section of the Toolbar before the submenu has two options.

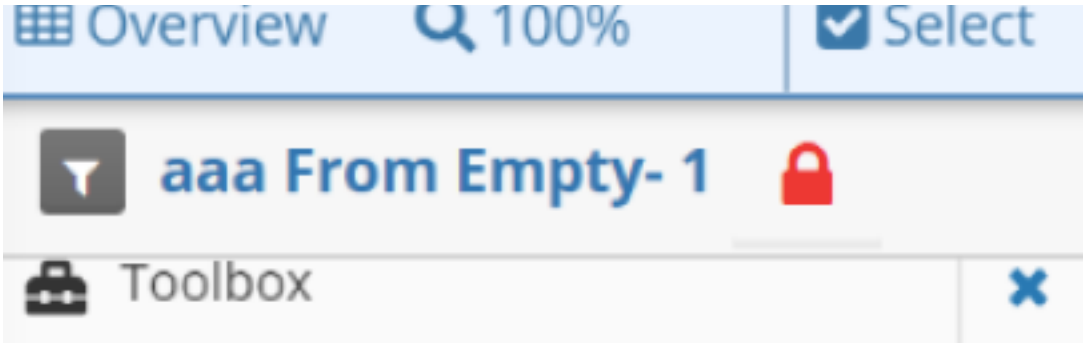
Import from Template – opens a popup with a list of Templates available to import directly into your diagram.



Submit for Approval – places your threat model in **read only** mode and notifies your administrator that the model is complete and ready for review. Your administrator will be notified via “Notifications” on the platform and it will show under Workflows. Submit for Approval enables multiple checkpoints along the threat mitigation process.

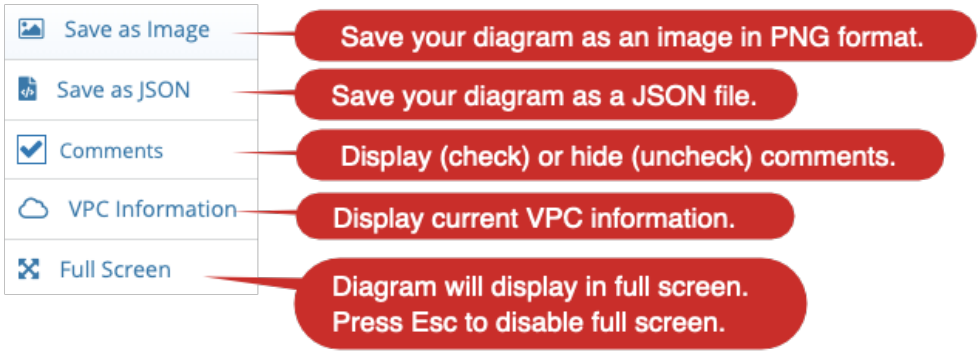


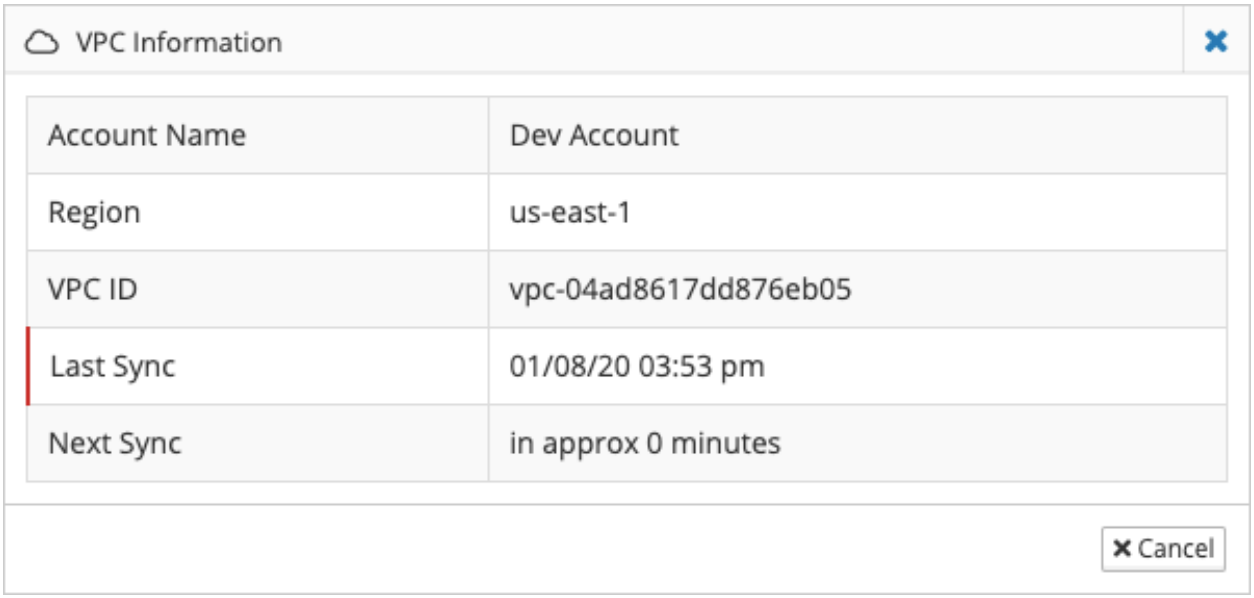
The threat model will remain in read only mode until it is returned for revisions. A red padlock  will be displayed next to the threat model name on the Diagram screen.



More Button

A Diagram drop-down menu with further options can be accessed via the  icon on the far right of the Diagram screen.

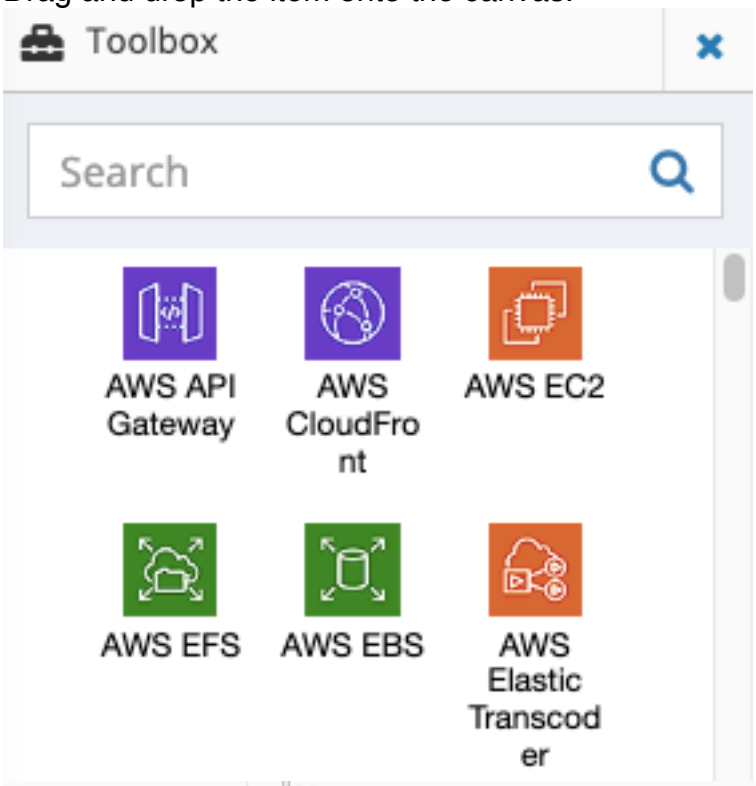


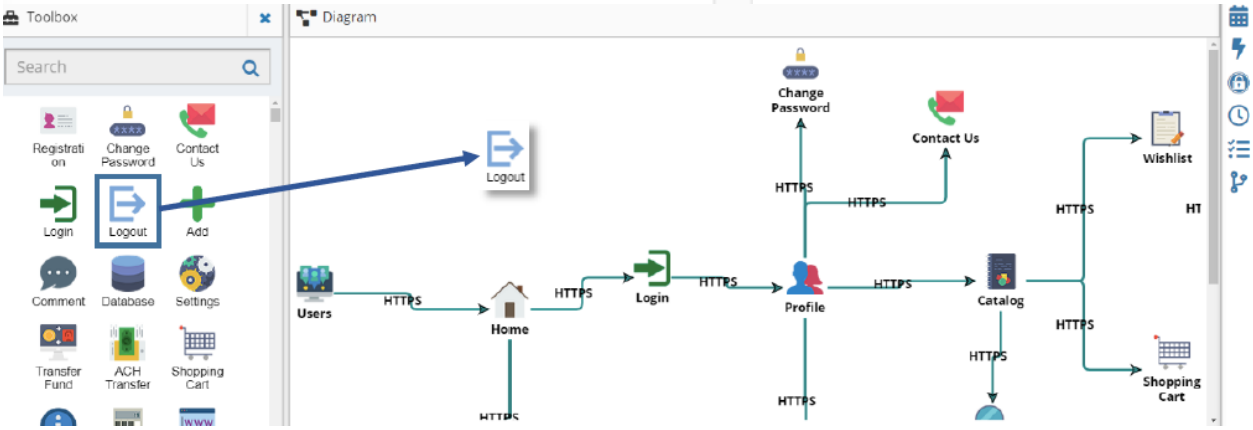


Working with the Toolbox

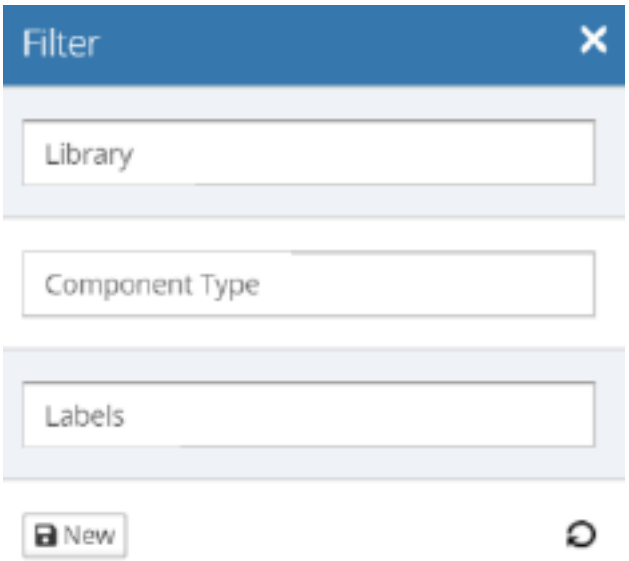
The Toolbox contains all the individual architectural features and components. When created in the ThreatModeler [Threat Intelligence Framework](), components can be added to any other threat model. Among others, the Framework compiles up-to-date information on threats identified by AWS (CIS), OWASP, CAPEC and WASC.

1. Use the Toolbox Search feature to filter what appears and locate the component.
2. Drag and drop the item onto the canvas.





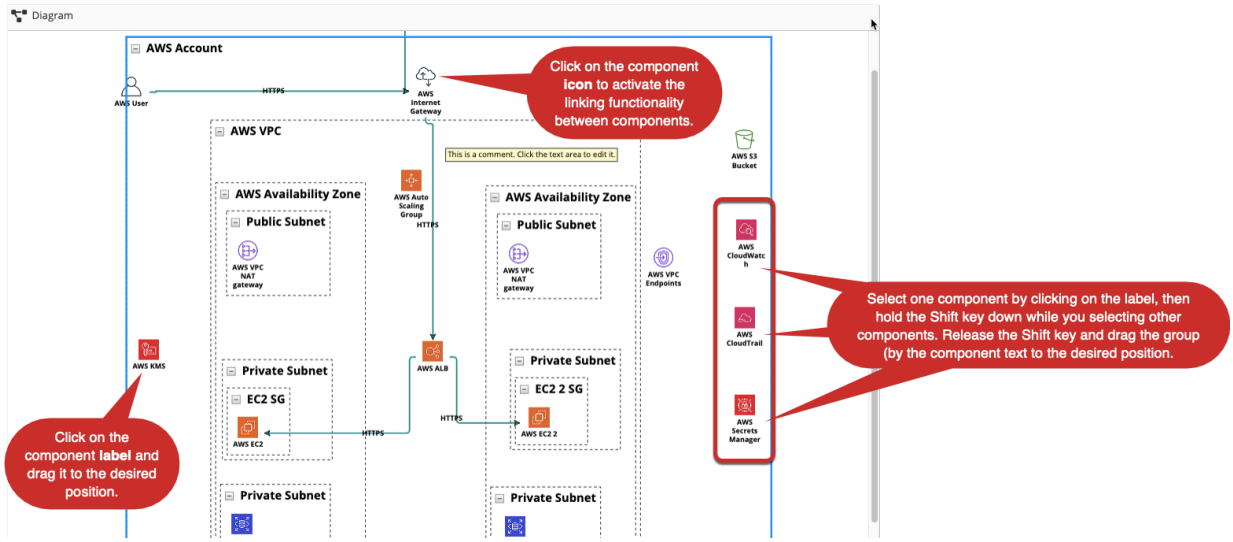
3. Use the Filter function to limit the components to specific component label, Library or type.



Working with the Canvas

The canvas is the workspace for your diagram. You can use the Toolbox and other features, such as Import from Template, to build your threat model.

Selecting Components Within the Canvas



1. Click on a component icon to view information about it in the General Properties window.
2. On the blank canvas, click, hold and keep your cursor still. Then, drag the components (each encased in a blue selection window that appears over all the components you want to select) to the desired position.

Linking Components

You can link components, which connects them via communication protocols.

Properties Sliding Panel

The sliding panel Properties toolbar to the right of the diagram canvas provides an expandable window with lists and options.

1. Click on the Sliding Panel Toolbar to Expand on options, lists and other information.
2. Click the same icon again to hide the window.

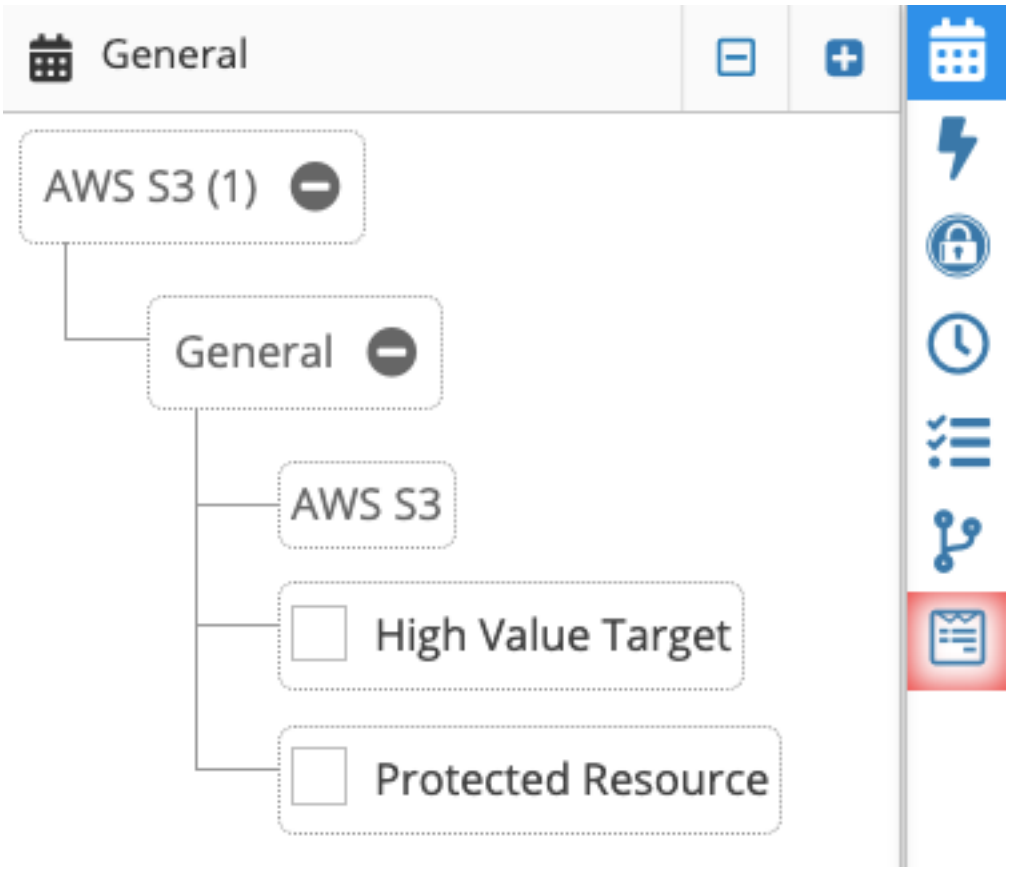
General Properties Window

Click on any component or Group in your diagram, and its properties will appear in the General Properties window. Add a property for any individual or set of canvas

components by clicking the  icon. You can add General Properties about the following elements:

Roles
Indicate the type of entity that has access to and uses a component. Role entities include people, operational components, cloud services, third-party systems or any other entity that interacts with a Component.
Widgets
Add Widgets to Components as a means to achieve a certain component state. Security requirements do not map to Widgets,
Data Elements
Add Data Elements to a threat model Component to indicate the type of information stored, manipulated or otherwise processed by that Component.
Components
For applications, architectural Components can include use cases, program packets, etc. For operational threat models, the Components can include servers, databases, laptops, communication towers, etc. Users can add Components using the General Properties icon.
Notes
Add Notes into the free text field to help communicate information to teams and stakeholders.
CPE ID
Standardized Common Platform Enumeration (CPE) IDs help users to identify and describe applications, operating systems and hardware devices that exist within an enterprise's computing assets.

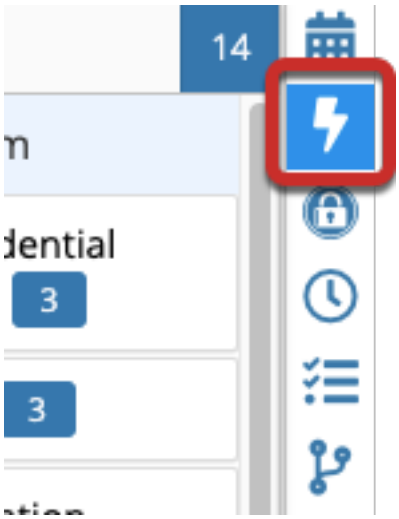
Adding the extra information allows ThreatModeler to identify additional threats that are particular to the respective information. Use the  and  icons to expand or collapse the General Properties tree.



Threats List

View all the threats associated with a particular component or Group. You can also view the threats with an Open status, by clicking the toggle at the top of the window.

1. Click on an area in the diagram, e.g. the component or Group, to filter the threats and show only those relevant to the Component.
2. Click on an open part of the diagram will clear the filter and display all the threats related to the diagram.
3. The Export function enables you to export Threats in an Excel file.

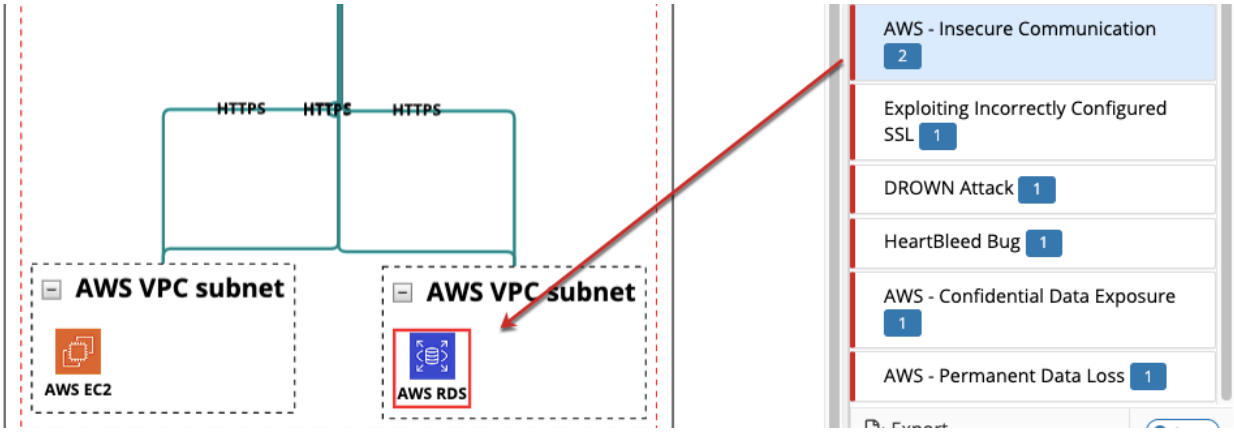


Threat List Elements

Click the Threats button to the right of the Diagram canvas to open the Threats List Slider. Threats are listed relative to the order in which they were identified.

Click on an identified threat in the Threat List Slider to identify the threat source(s) on the diagram Canvas, highlighted with a red box. Communication link protocol names are highlighted in red text.

1. Click on a component or communication link included in the Diagram canvas to filter the threat list to display item details. If the user selects multiple items, the filter bar is removed from the Slider display.

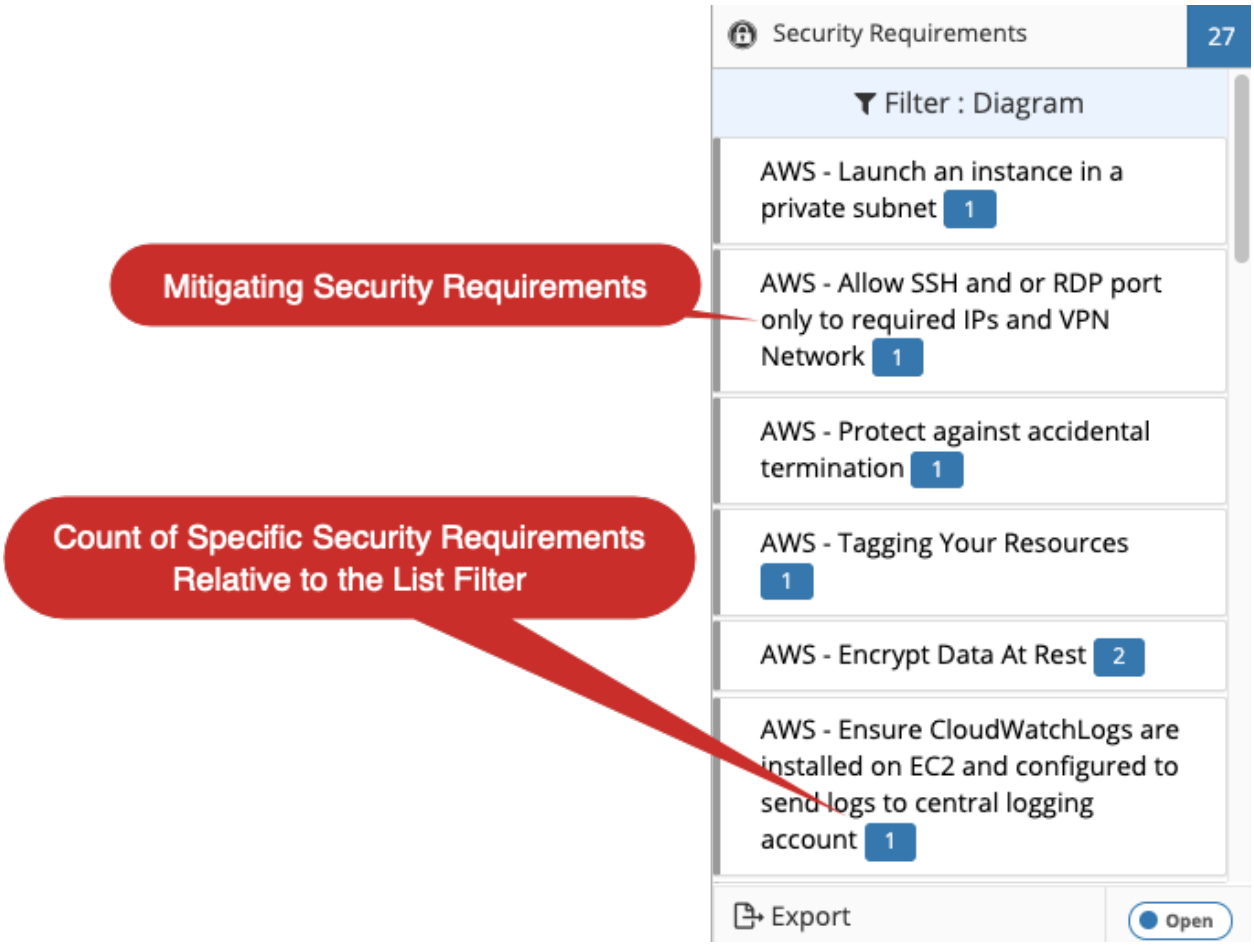


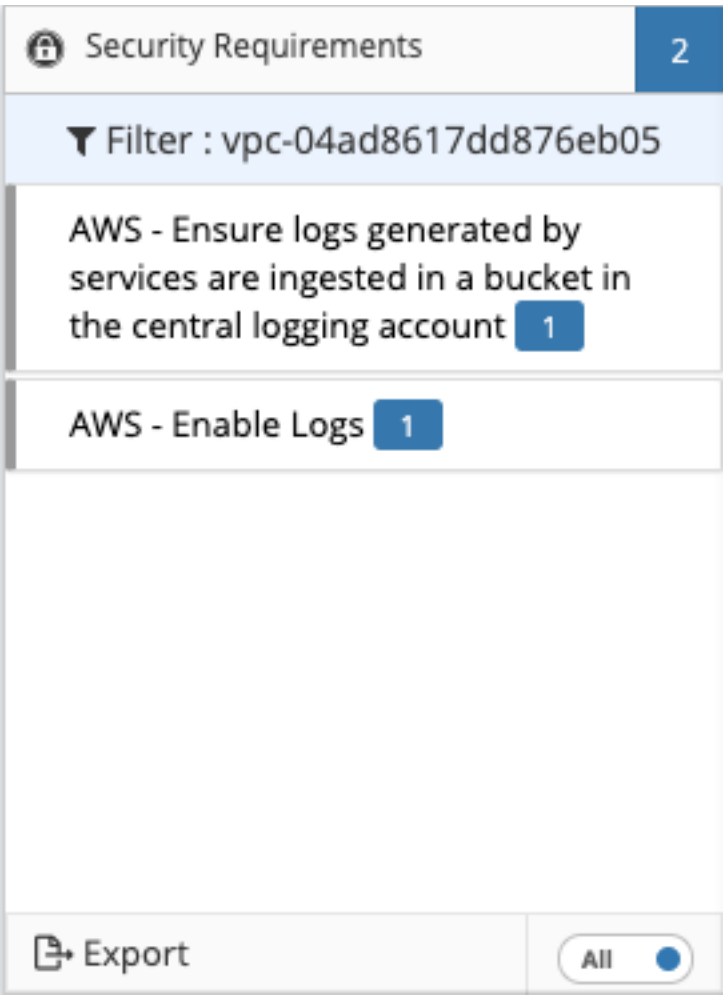
Security Requirements List

Shows all the security requirements associated with the selected component or Group. Filter enables you to isolate components in the diagram. While Security Requirements are listed in order to when the corresponding threats were identified, the first in the list will be based on the type threat model selected when it was created.

Clicking on an individual security requirement in the Security Requirement List slider highlights the architectural component(s) or communication link(s) on the diagram canvas with a red box. Communication link names are highlighted in red text.

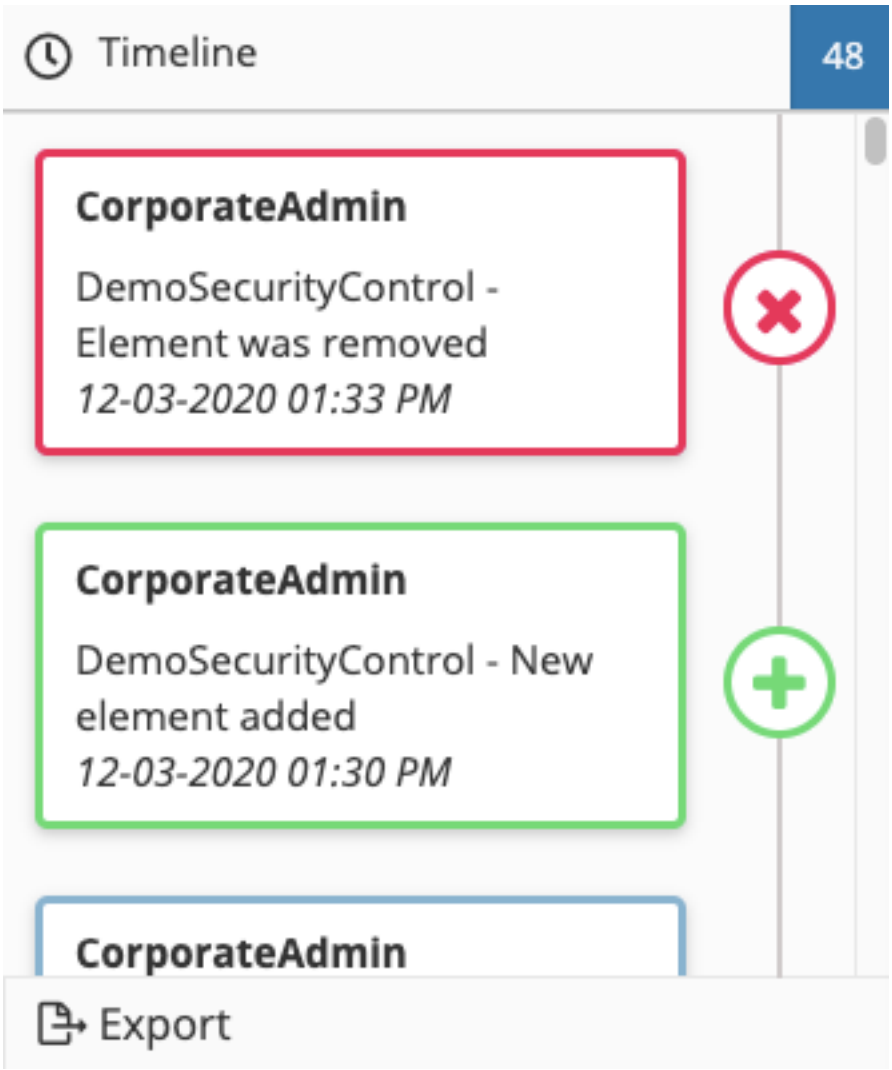
1. As with the Threats List, you can choose to only view the open security requirements by toggling between Open and All at the top right.
2. Click on an area in the diagram, e.g. a component, to Filter the Requirements to the area you've selected.
3. Click on an open part of the diagram to clear the filter and display all the threats.


Security Requirements
27
Filter : Diagram
AWS - Launch an instance in a private subnet 1
AWS - Allow SSH and or RDP port only to required IPs and VPN Network 1
AWS - Protect against accidental termination 1
AWS - Tagging Your Resources 1
AWS - Encrypt Data At Rest 2
AWS - Ensure CloudWatchLogs are installed on EC2 and configured to send logs to central logging account 1
Export
Open
Mitigating Security Requirements
Count of Specific Security Requirements Relative to the List Filter



Timeline

Provides a running list of all the instances when the threat model is edited. View the revisions made, by who (username), with a date and timestamp.

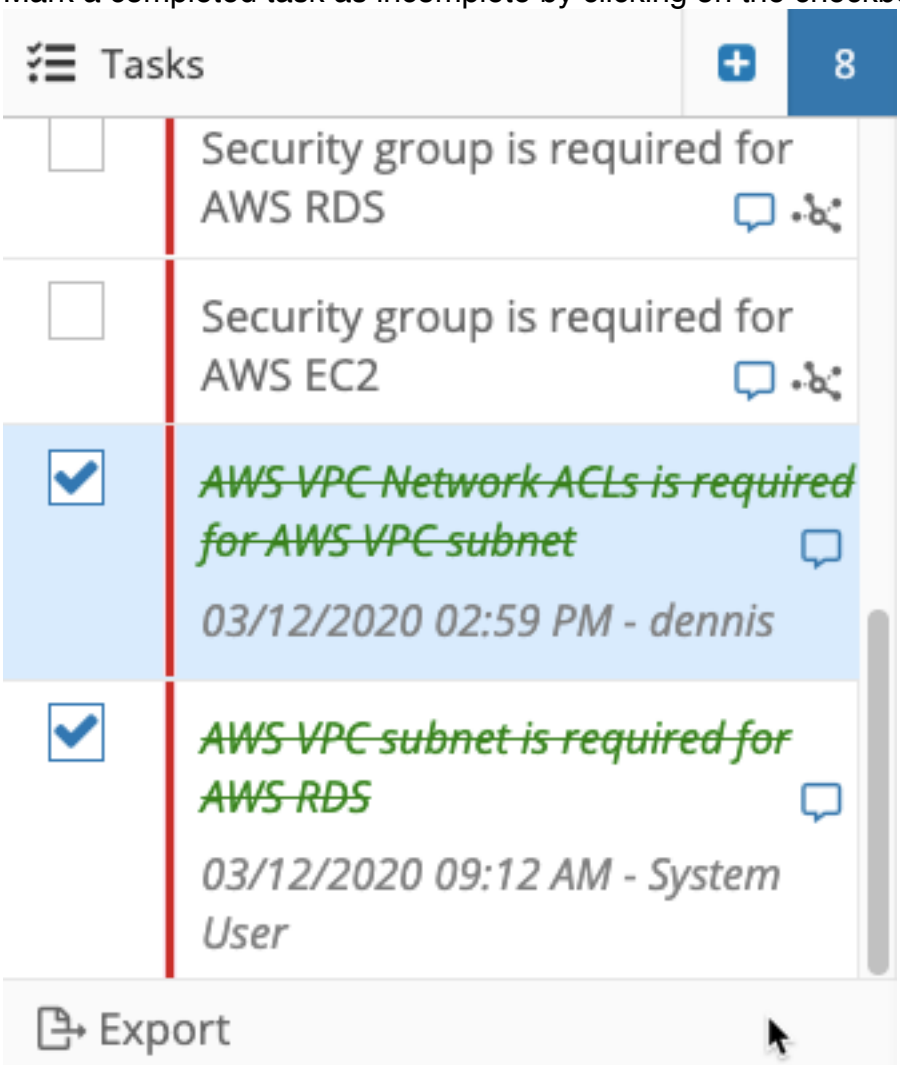


Task List

Review a backlog of tasks associated with a threat model.

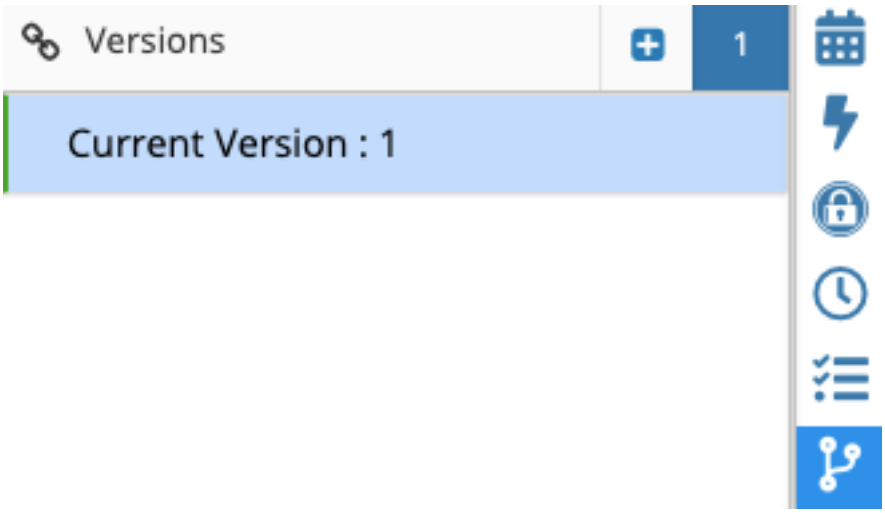
1. Add a task by clicking the icon.
2. Check tasks off as complete when appropriate.
3. Execute a task by clicking on the icon.
4. Comment on a task by clicking on the icon.
5. Show a task is complete by clicking the checkbox next to it.

6. Mark a completed task as incomplete by clicking on the checkbox again.



Version Log

View the current version on which you are working. The Version log also shows the list of versions for your threat model. You can add a new version by clicking the plus icon at the top right.



Create Your First Threat Model

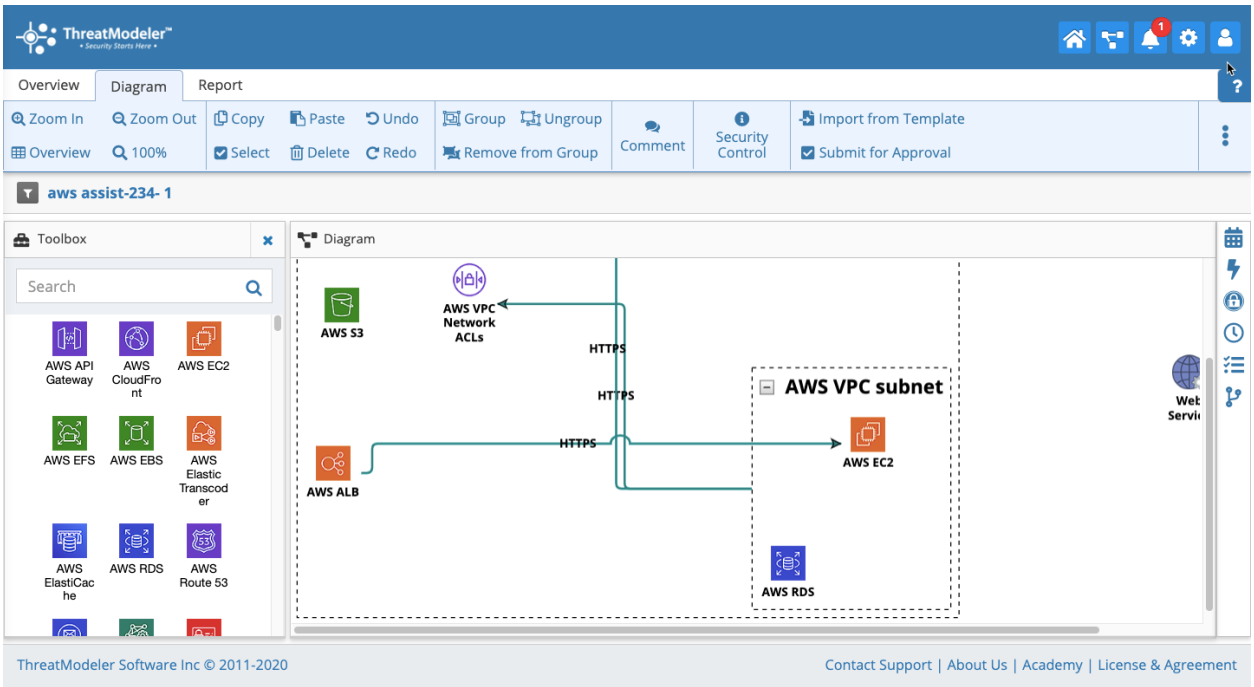
Generate accurate, actionable outputs with ThreatModeler. ThreatModeler uses process flow diagrams (PFDs) that enable you to think like a hacker, illustrating how to move through application use cases within an operational environment. PFDs lend themselves to visualization and make it easy to understand how users interact with a system.

After dragging and dropping pre-defined components onto the diagram canvas and arranging them, ThreatModeler's Intelligent Threat Engine™ automatically analyzes the diagram. The Intelligent Threat Engine generates outputs for all stakeholders – including C-Suite, DevSecOps teams and QA – enabling collaboration. ThreatModeler is ideal for today's fluid, CI/CD pipeline, highly interconnected systems, plus technology deployment environment.

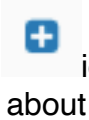
Three Basic Steps to Threat Modeling

Creating a threat model in our platform includes three steps:

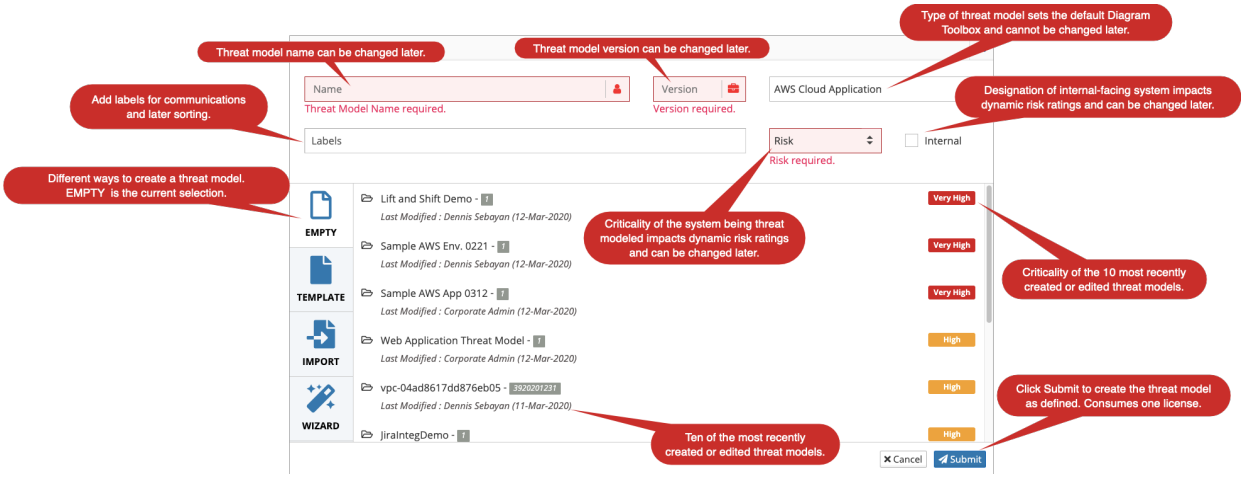
1. Place pre-defined Components onto the Diagram canvas. Out-of-the-box, ThreatModeler comes with hundreds of architectural components, communication protocol definitions and property definitions.
2. Add the appropriate communication protocol links between components.
3. Define specific properties for components.



Creating a New Threat Model

1. The first thing you will do is navigate to the primary Threat Models screen.
2. Click on the  icon. The “Create a new threat model” screen is displayed.
3. Input details about the Threat Model:
   - Name (Required) – can be edited later.
   - Version (Required) – can be an alphanumeric value, but it must be unique within the organization’s ThreatModeler instance.
   - Risk setting – based on the criticality of the application you’re modeling, Risk setting contributes to calculating the Dynamic Risk Ratings of automatically identified threats (contact support@threatmodeler.com to inquire about this configurable option).
   - Type of Application – default type is an AWS Cloud Application. This field *cannot* be edited at a future time. The Application Type determines the component library that is presented to the user on the Diagram screen. The user always has the option to remove the filter once inside the diagram.
   - Labels – add one or more labels from the drop-down list, which are useful for sorting large lists of threat models and communicating to collaborators. A free text option allows you to input values that aren’t on the list.
   - Whether your model is internal or external facing – the default (unchecked) setting is external. This setting contributes to calculating the Dynamic Risk Ratings of automatically identified threats.

Create a Threat Model From Empty, Template, Import or Wizard



Create a Threat Model Using Empty

Advanced Users can create the threat model from Empty (a blank process flow diagram).

1. Click on the Empty icon.
2. Fill in the required and optional fields.
3. Clicking the Submit button will consume one ThreatModeler license.

Create a Threat Model From Import

With ThreatModeler, you can import process flow diagrams created in Visio and LucidChart and generate accurate, actionable output.

1. From the Threat Models primary screen, click  to open the New Threat Model dialog box.
2. Click on the Import icon.
3. Browse and select the file to import.

4. Click the validate button. ThreatModeler will scan the file to ensure compatibility for diagram creation.
5. If validation is successful, then click Submit, which will consume one ThreatModeler software license.

Diagram Screen Displays Imported Components Pre-Arranged on Your Canvas

After clicking Submit, you will navigate to the Diagram screen. The Template will be on the canvas and set in Collection Group. You can also Ungroup the Template to modify the threat model. All changes are saved automatically.

In addition to the Template components laid out on your canvas, you can:

- Add components.
- Make changes to existing Templates.
- Add general properties and tasks to the threat model.

Create a New Threat Model using the Template Button

Users can store standard diagram portions as Templates for reuse, enabling organizations to scale easily. Use existing Templates to create new threat models or add them to existing threat models.

1. Click on the Template icon.
2. Select the Template by entering search terms and selecting it from the drop-down list. You can also use the 

button. Images of the Template are on the right side of the drop-down list.
3. Complete the dialog box as you would with the other options.
4. Clicking Submit consumes one ThreatModeler license.

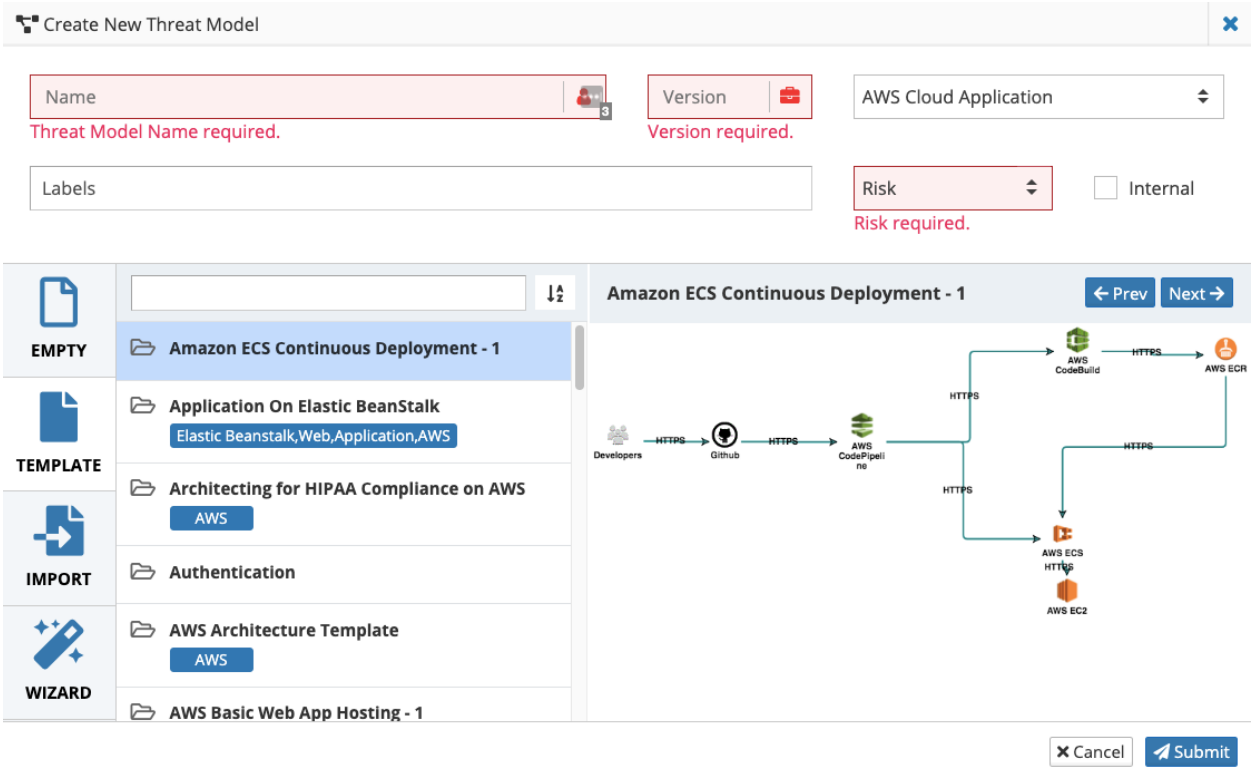


Diagram Screen Displays Template Components Pre-Arranged on Your Canvas

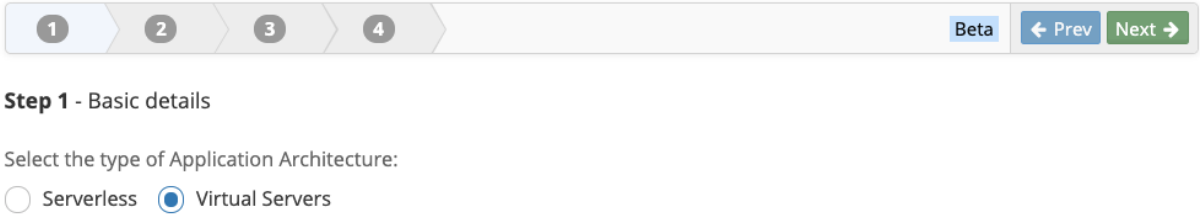
After selecting the Template, you will navigate to the Diagram screen. The Template will be on the canvas and set in a Collection Group. You can modify the threat model diagram by:

- Ungrouping the Collection Group.
- Adding components.
- Adding general properties and tasks to the threat model.

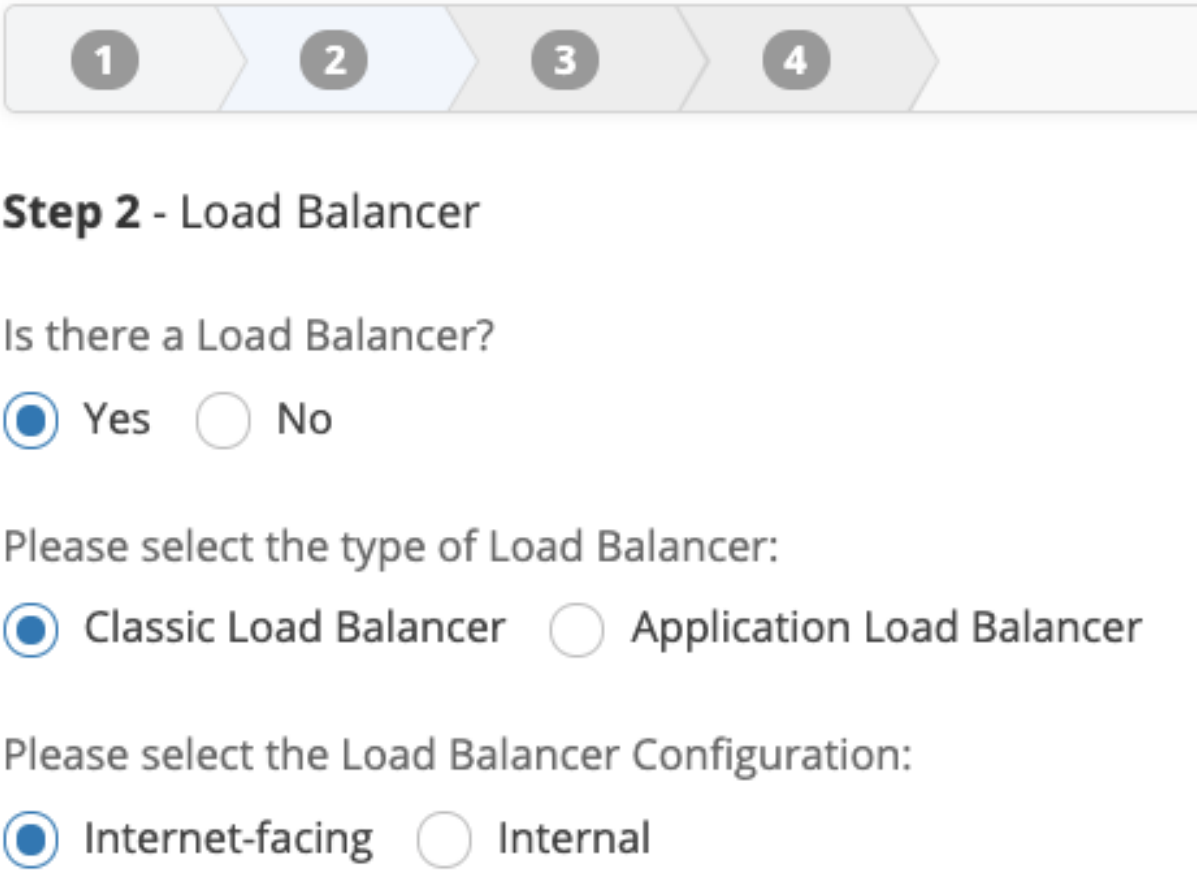
Create a Threat Model using the Wizard

ThreatModeler makes it easy for users to threat model for AWS cloud deployments by completing a brief questionnaire about your underlying architecture.

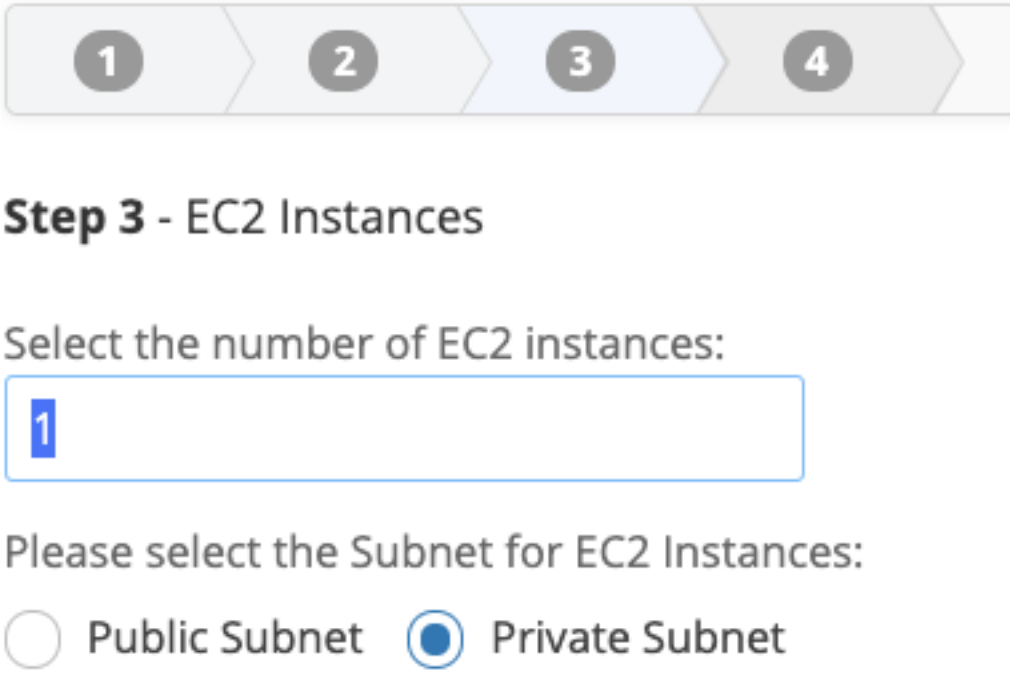
1. From the Threat Models primary screen, click  to open the New Threat Model dialog box.
2. Click on the Wizard icon.
3. The Wizard is available when the AWS Cloud Application is selected. Once selected, a dialog box will display an AWS-specific questionnaire.
4. The first question is about the type of Application Architecture, with Virtual Servers as the default selection. The default selection is shown here.



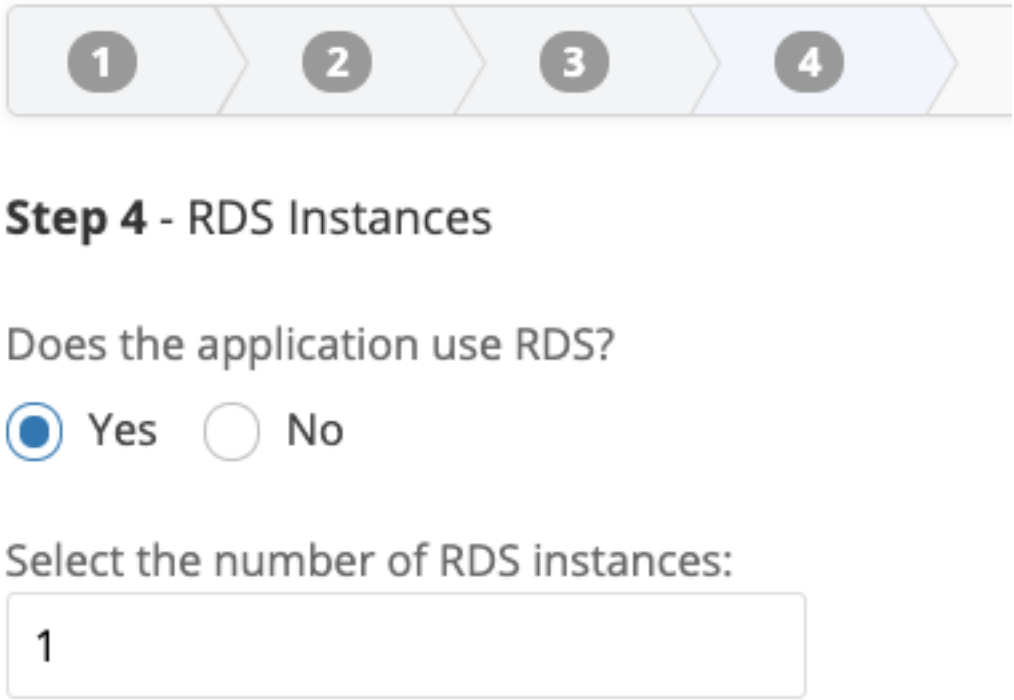
5. Question two asks whether or not there is a Load Balancer, and if so, how many. Default selection is shown here.



6. Question three asks for the quantity of EC2 instances in the deployment, and whether they will be contained in a private or public subnet. If user select Public Subnet, ThreatModeler warns that it is a good idea to contain EC2s in Private Subnets.



7. The final question asks if the application uses RDS instances and, if so, the number of instances.



8. After answering the final Wizard question, click Finish. One ThreatModeler license will be consumed.

EMPHASIS BOX: The same Wizard is available for users who select Serverless in question one.

Diagram Screen Displays Wizard Components Pre-Arranged on Your Canvas

After clicking Submit, depending on your answers to the Wizard questions, ThreatModeler will create a baseline architecture for you on the Diagram screen. You can also Ungroup the Template to modify the threat model.

In addition to the baseline architectural components laid out on your canvas, you can:

- Add components.
- Make changes to existing Templates.
- Add general properties and tasks to the threat model.

Placing Components

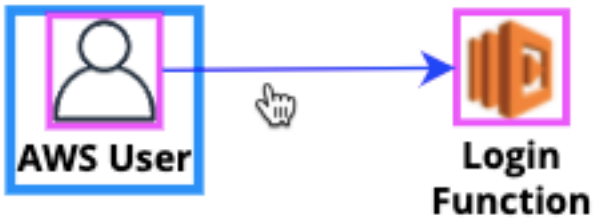
Once in Diagram screen, drag pre-defined architectural components from the Toolbox and place them relative to the “process flow” being threat modeled.

- Applications will include use cases, program cases, etc.
- Operational threat models will include servers, databases, laptops, communication towers, etc.

Adding Communication Protocols Between Components

The next step is to add communication protocols linking various features.

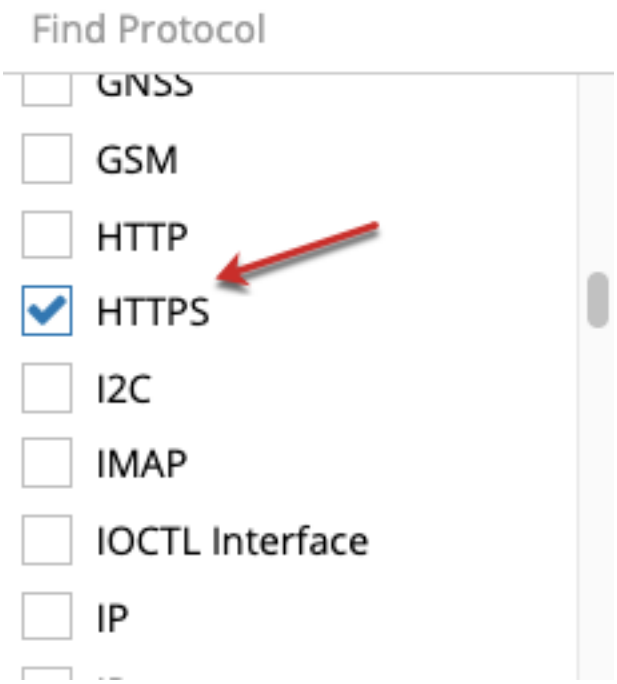
1. Click and hold the first component icon that was placed on the canvas. ThreatModeler automatically creates an arrow for use.
2. Drag the blue arrow to another component icon.



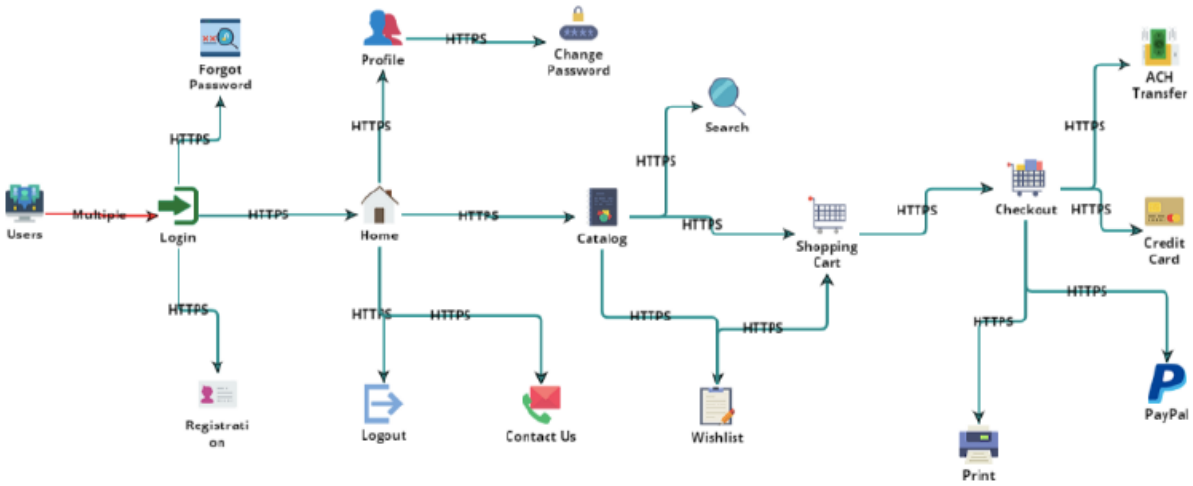
1. Drag the blue arrow that appears across to the second component icon.
2. Your two components are now linked with a communication protocol.

Select Communication Protocol Type

1. The default communication protocol is HTTPS, though ThreatModeler allows for multiple communication protocols.
2. If you want to change or add more protocols, right-click on the arrow link and select the protocols to include.
3. If you want to remove the default HTTPS protocol, you need to uncheck it from the menu.



4. For this example, all our links will use the default HTTPS protocol. Continue adding communication protocols between the threat model components according to the architectural design.
5. Input text for the communication protocol needed, ThreatModeler will hone-in on the communication protocol as you type.



Working with Groups

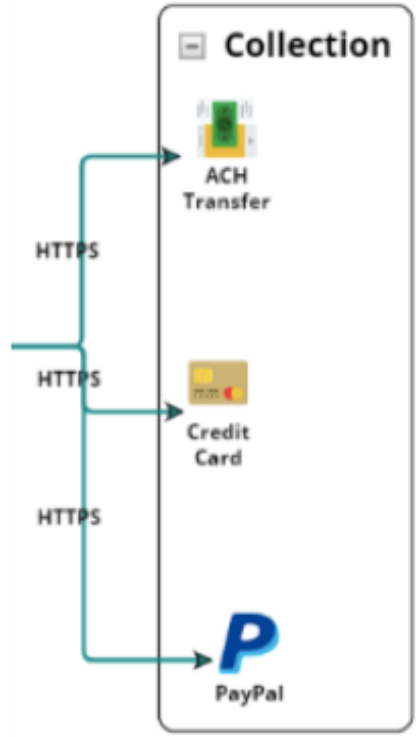
Grouping is a functionality that allows you to collect components and make changes that affect the entire Group of components.

Types of Groups

Some types of Groups, such as Trust Boundaries, can affect the threats and security requirements generated for that Group. Other types of Groups, like Collections, are primarily used to make your threat model diagram organized and easier to understand. There are three types of Groups:

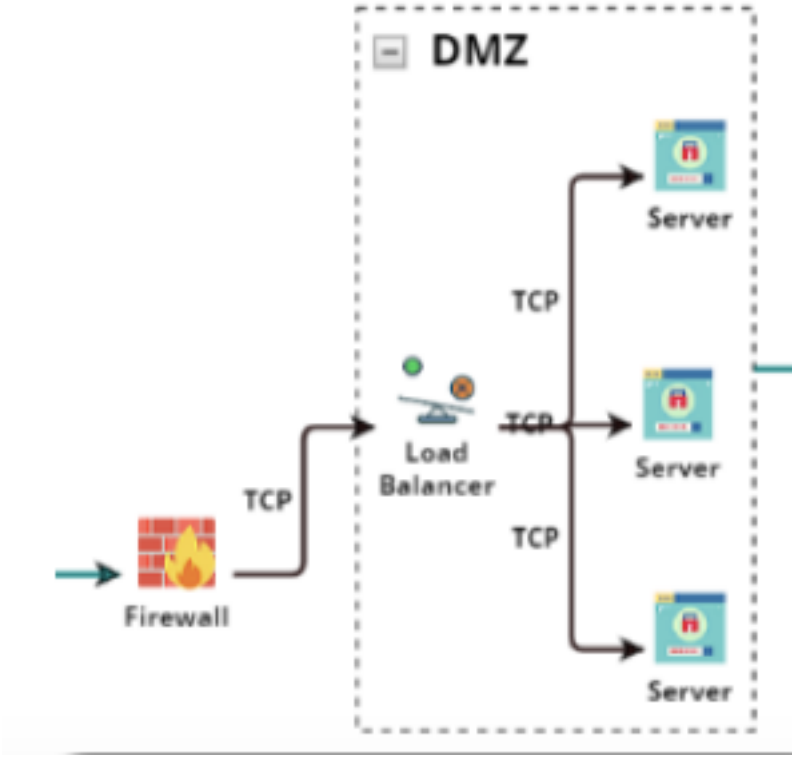
Collection

The default Group type is a collection. These are simple diagraming boxes which allow users to move, position or hide related components simultaneously. Collections have no innate features or threats associated with them.



Trust Boundary

Trust boundaries indicate a logical trusted zone for multiple components inside of them, for example, a DMZ, VPC etc. It is understood that the components contained within a Trust Boundary are logically placed.

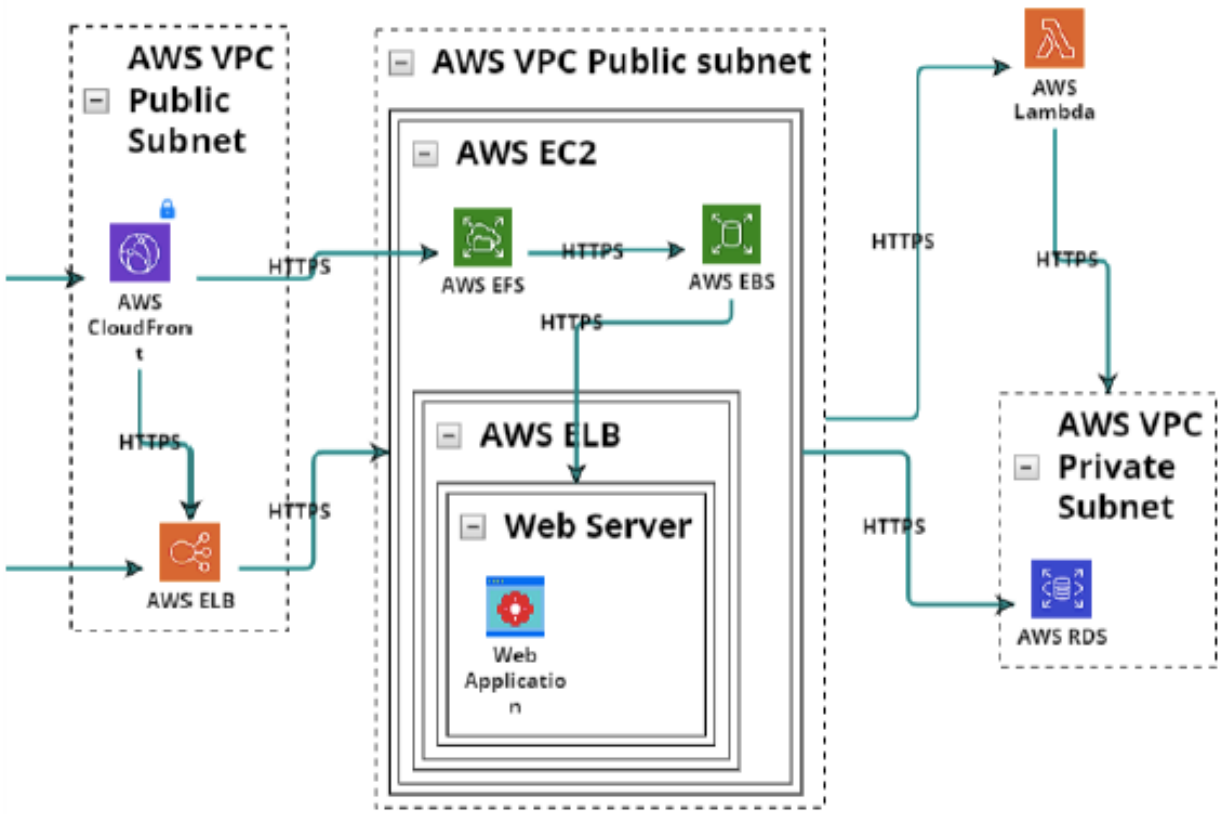


Container

- Containers show a logical grouping of components. For example, a data center on the cloud can have many individual components – each of which can be included in one or more containers – to indicate that these items are “contained” in a logical manner.
- However, Components from the Toolbox can be reflected as Containers as well. These Containers take on the properties of a Component selected from the toolbox.
- The functionality of the containers is the same as that of the associated component.
- Containers may have innate threats or features associated with them.

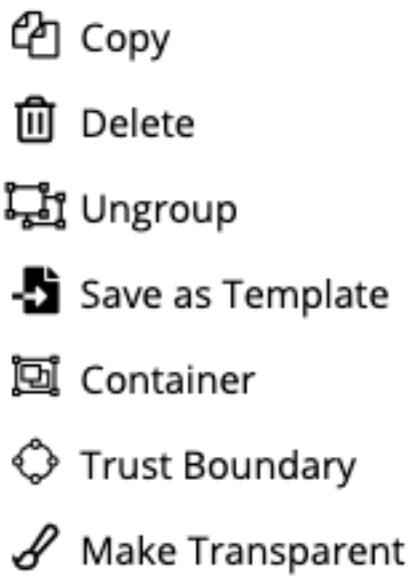
Behavior Common to All Group Types

Certain behaviors are standard across each of the Group types. Communication links may be formed between a grouped component and non-grouped component, between the Group and non-grouped component, or between Groups.



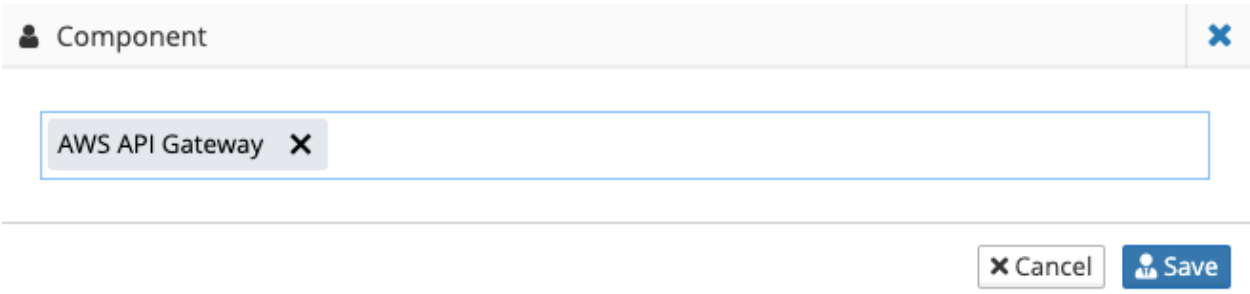
How to Create a Group From a Set of Components

1. On the threat model Diagram canvas, select the components by clicking and dragging them.
2. Alternatively, you can SHIFT-click or CTRL-click each component to select them. Communication links between selected components will automatically be added to the Group.
3. Select “Group” from the toolbar. The selected components will be grouped as the default group type, Collection.
4. You can also create a group without selecting any component and add components to it later on.
5. Right-click on the Group to open a drop-down menu. From this menu, you can:



- Copy or delete the Group.
- Ungroup.
- Save Group as a Template.
- Change the type of Group from the default (Collection) to a Container or Trust Boundary.
- Make the Group Transparent.

Setting Containers or Trust Boundaries



1. On the Collection, right-click and select Trust Boundary or Container. A popup screen will allow you to choose the specific Component for a Container or Trust Boundary. Select Trust Boundary. A popup dialog box opens.
2. Click in the dialog box field to expand a drop-down list. Select Trust Boundary.
3. Click Save and the Group type on the diagram is changed to a Trust Boundary.
4. To rename the group, double click the name, which will not change the Group or the component you selected.
5. You can minimize a Group by clicking the icon next to the Group name.

Setting Containers is Similar to Setting Trust Boundaries.

1. Starting with a Collection, right-click the Group.

2. Choose Container from the popup menu and the Container dialog box will open.
3. Click in the dialog box and, from the drop-down menu, select the Container definition. Input the definition name and ThreatModeler will automatically filter the list per user type.
4. Click Save.
5. Containers behave on the diagram just like other Toolbox components. Users can assign additional properties to them.

Maneuvering Entire Groups

1. Maneuver a Group like you would a component by clicking and dragging the entire Group.
2. Resize a Group by repositioning one of the components inside it. If you have only one component in your Group, you cannot resize it.
3. Ungroup by simply selecting the undesired group and clicking Ungroup on the Diagram toolbar.
4. To remove a component from a Group, selecting it and choose “Ungroup” from the toolbar. You can now drag that component out of its Group.
5. Once removed from a Group, click and drag a component to put it into a different Group.
6. Once it is completely inside and arranged in a new Group, you can release the component. You will be asked to confirm the action before the component belongs to the new Group.

There Are No Barriers to Linking Components

Groups do not provide any barriers to linking components. Whatever the communication protocol lines you need for your model; the Group functionality will not prevent you from creating them. You can draw communications protocols:

- Between Groups to link them.
- From components to Groups.
- From a component in one Group to a component in another Group.

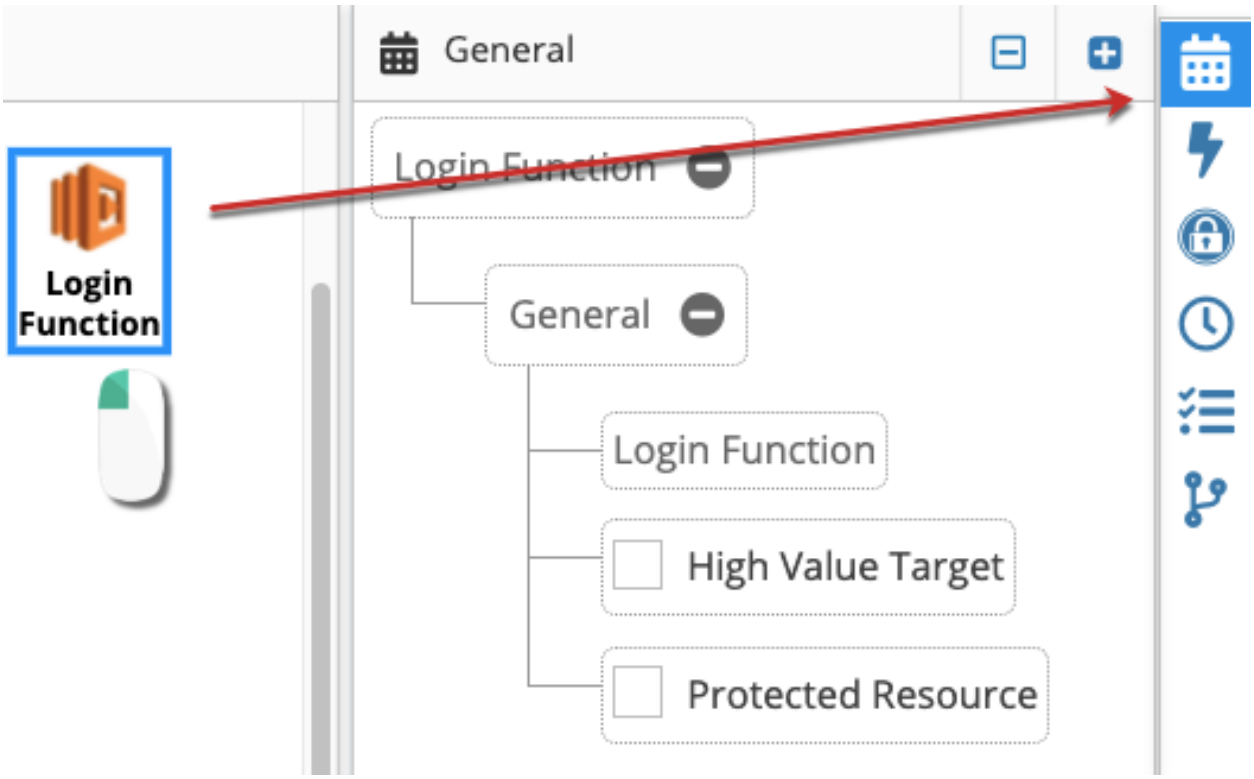
Adding Properties to Components

The final step to building a basic threat model is to add information or properties to individual components.

Example One – HTML Form that Communicates with a Database Backend

Login component will present the application user with an HTML form that communicates with a database backend.

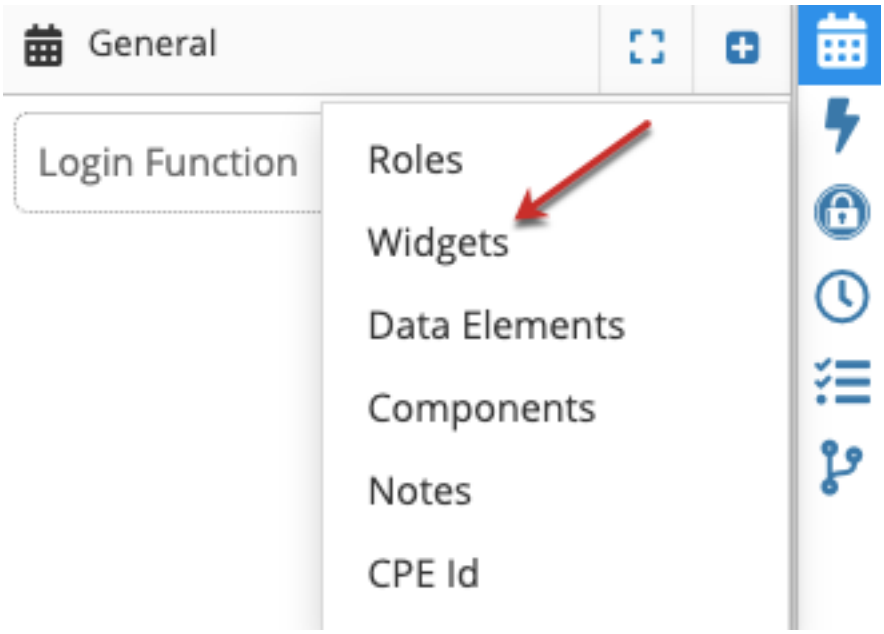
1. Click on a component to select it.



2. Click on the General Properties icon on the right to open the sliding panel.

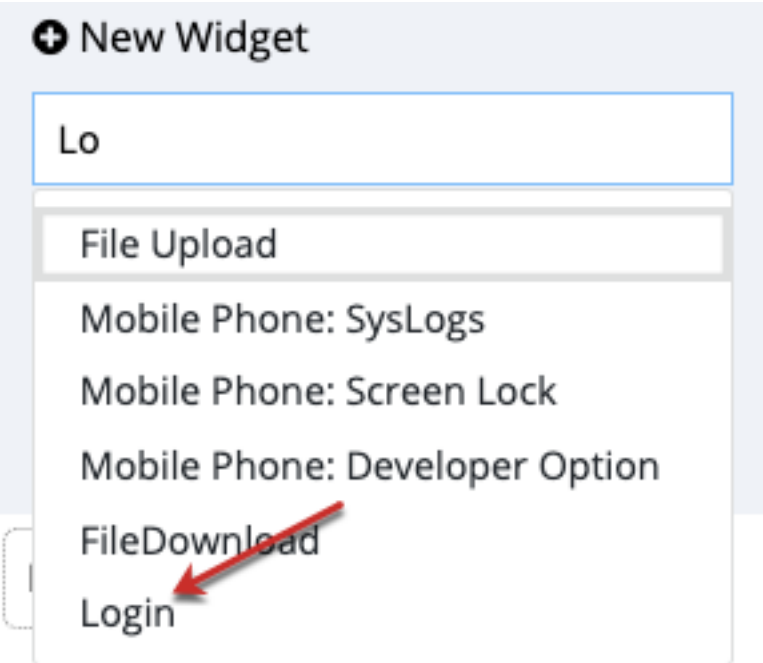
3. Click the Add button.

1. From the use case requirements, we know the login page needs to be an HTML form that has backend access to a database. On the popup menu, select Widgets. The purpose of widgets is to enable a component to achieve and maintain a state. The widgets list contains a number of objects from which to use, including cookies, PDFs, email, XML messages and more.

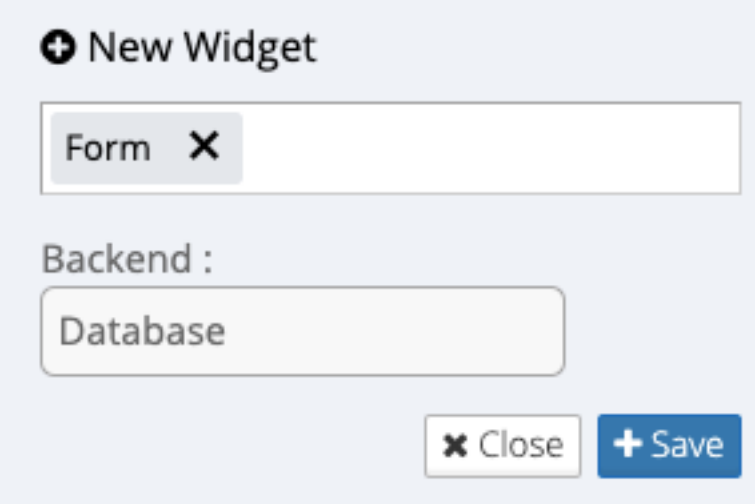


.

2. In the New Widget field, select Login.



3. Navigate to the General properties panel and click the  icon.
4. Again, choose Widget from the menu.
5. Select Form from the list.
6. In the Backend field, select Database from the drop-down list.



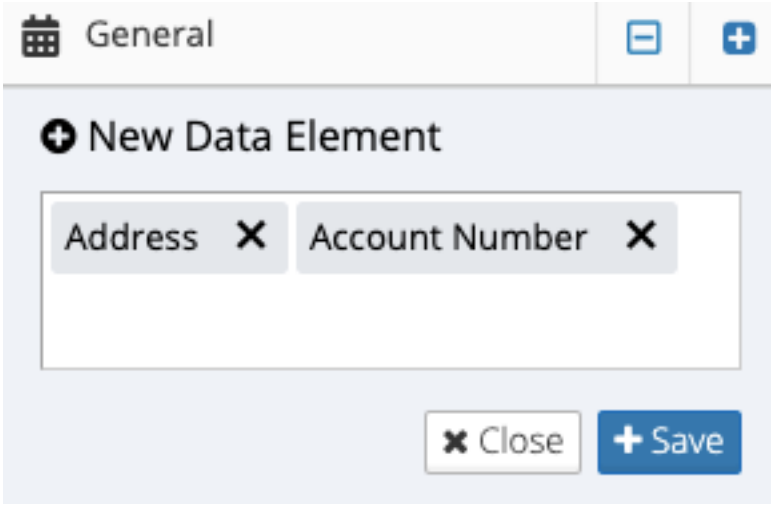
7. Click Save. You now have Form listed as a widget in the General Properties.

8. You can add the same property to multiple components at once by selecting the components and then using the general properties panel.
9. Continue adding various properties, e.g., Roles, Data Elements, etc., to the Diagram components as needed. Once the last property is added, your threat model is finished.

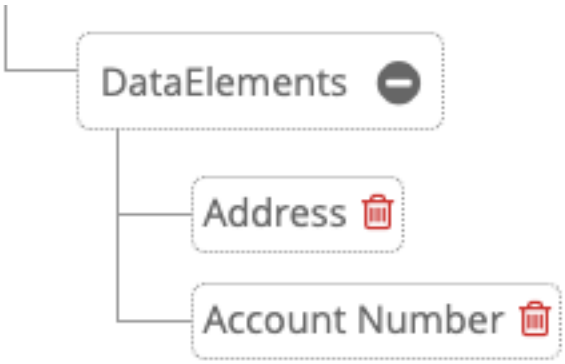
Example Two – Data Elements

Another property we can add to our model is a Data Element. For example, on a website registration page, a user may need to input personal information. We can add those data elements to the registration component.

1. Select the Registration component and click the  icon on the general properties panel.
2. Choose Data Elements from the menu.
3. Choose the personal information you want to add.
4. Add multiple items at once by typing the name of each element and selecting it from the drop-down list.



5. Click Save.
6. Remove the general properties you have added by clicking the red garbage can icon next to the property.



Example Three – Placement of Cookies

In this example, for the application to function properly, the Login feature will:

- Place a cookie on the user's computer.
- Change the session ID.

We can add both architectural element widgets by taking the following steps:

1. Select the Login component.
2. Click the icon from the Widgets bar. The Widgets dialog box will open.
3. Select Cookie from the drop-down menu.
4. Before saving, click again in the widgets box to access the drop-down menu.
5. Click the Session widget. Both widgets will now be in the widgets bar in the dialog box.
6. These widgets do not need to communicate with the backend. Leave the interaction menu item as None.

Note on Adding Properties

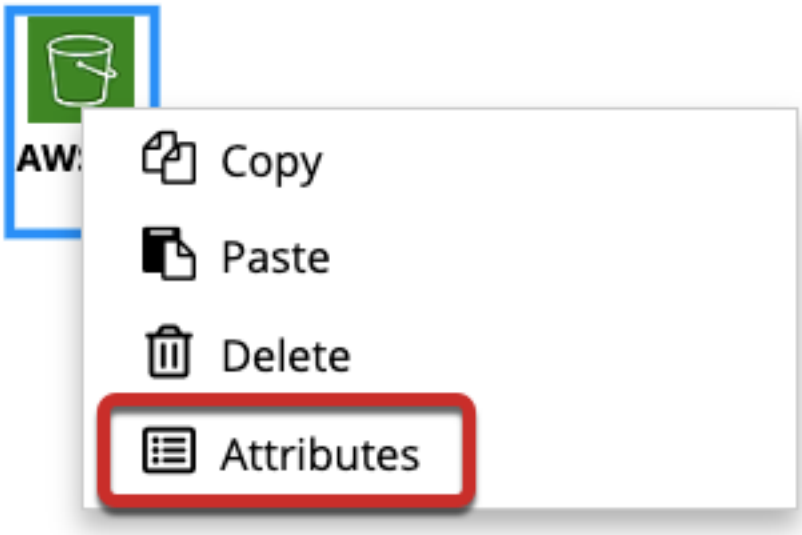
Assigning properties to the canvas components may increase the number of threats identified by ThreatModeler. Carefully review all of your components after your model is built and add any relevant properties.

Working with Attributes

Attributes are a type of Property that describe how a particular type of component may be running or operating within a system. Attributes are component specific. While ThreatModeler comes pre-packaged with common attributes, users can access the Threat Framework to define additional attributes based on their organizational needs.

To assign one or more attributes to a specific component on a threat model diagram:

1. Right-click the intended component on the Diagram canvas and select Attributes from the popup window. A separate Attributes popup window will open.



2. Toggle the desired attributes from the list, which ThreatModeler dynamically loads based on the selected component type, between YES and NO.
3. Click the Update button. ThreatModeler will automatically identify relevant potential threats associated to the selected attributes and add them to threat model outputs.

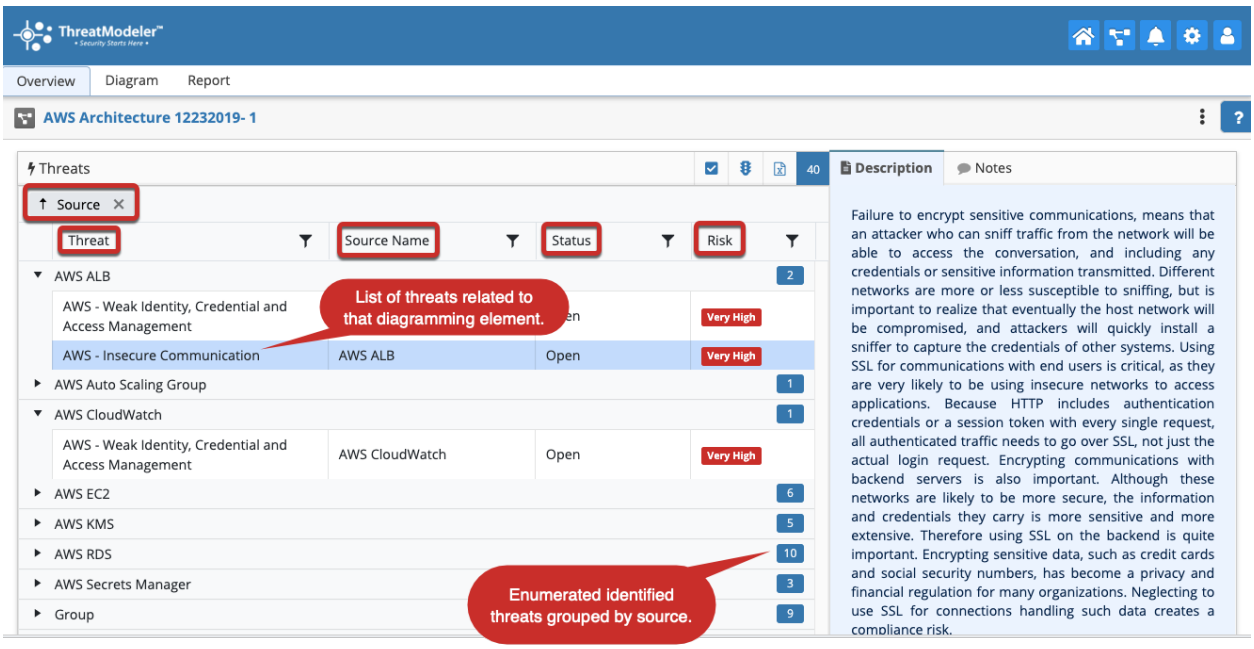
Overview Screen

When you double click on a Threat Model, you are navigated to its Detail views. All the details of the model can be found across three tabs:

- Overview
- Diagram
- Report

Overview Tab Outputs

Clicking on the Overview tab navigates you to detailed on-screen threat model outputs automatically generated by ThreatModeler.



Threat Definition

A malicious or careless act carried out by a bad or negligent actor to compromise an attack surface. Once compromised, further damage, theft or disruption to the data objects stored therein can occur. Certain characteristics associated with the Threats are viewable:

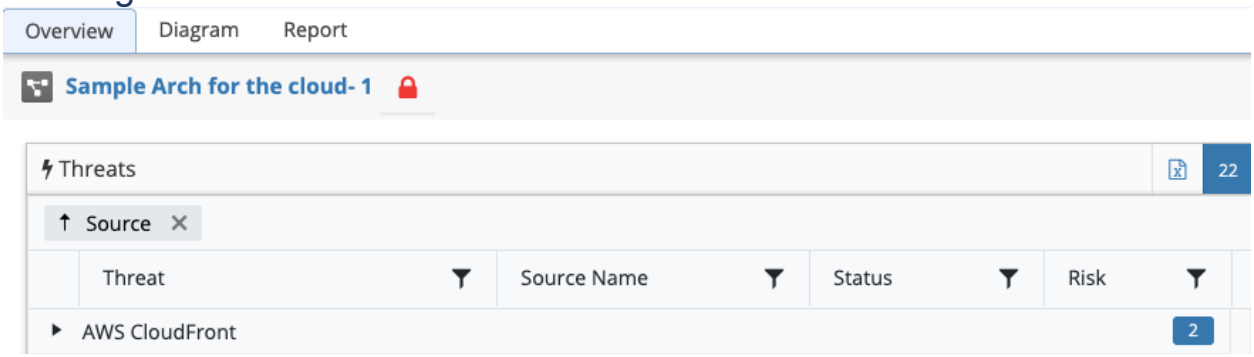
- Source – the component that is tied to the threat.
- Status – indicates whether or not the threat mitigation is open or closed
- Risk – describes the risk level, from Very Low to Very High
- Issue – when AWS is integrated with Jira, the field allows you to filter Issues based on a ticket ID.

1. Click the  icon to open a source Group with a list of threats related to that element.

2. Click on the  icon to close the Group list.

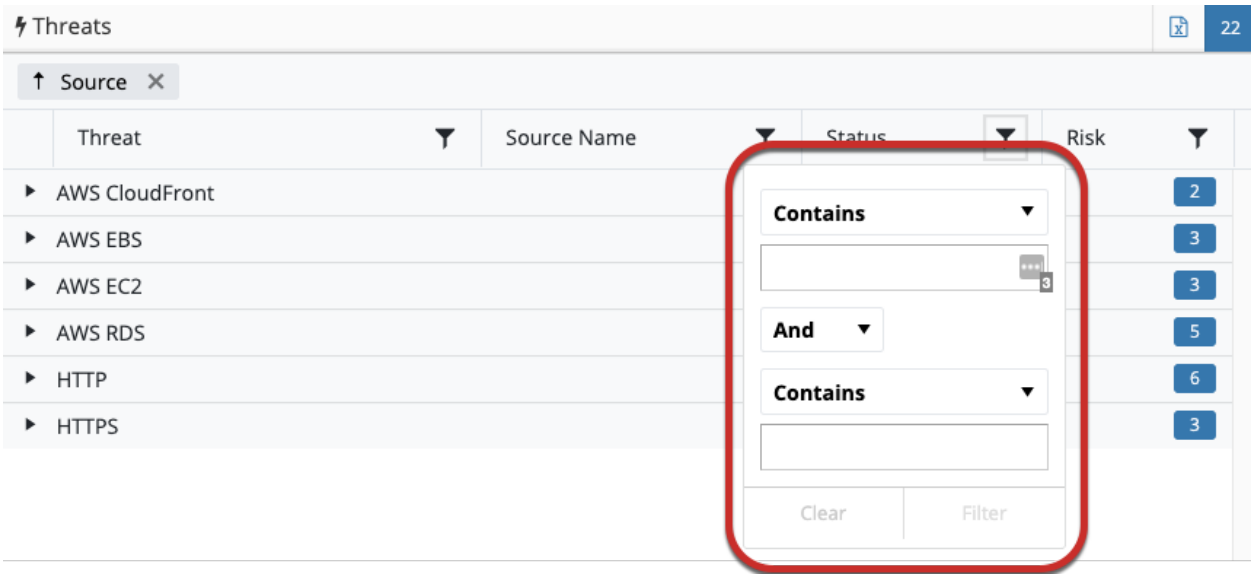
Description and Notes – Click on a threat to view its Description and add notes to any of the panels about Threats, Security Requirements and Test Cases.

Filtering the Threats List

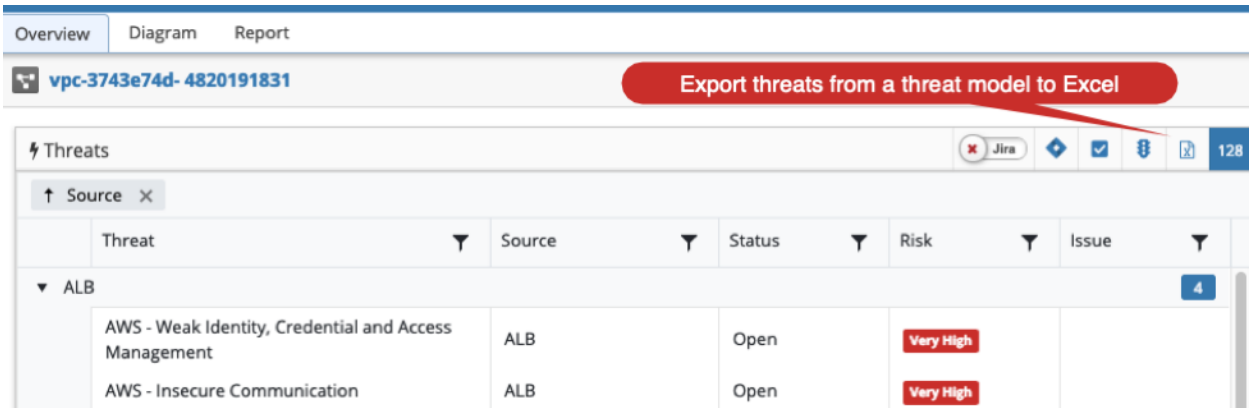


You can sort the threat list by any of the column titles (Threat, Source, Status, Risk). You can also move the column titles to different areas along the screen. To filter the Threats List,

1. Click on the filter  icon.
2. Enter text in the Contains field(s).
3. Click Filter.



4. To export the threats form a threat model to Excel, click on the  icon.

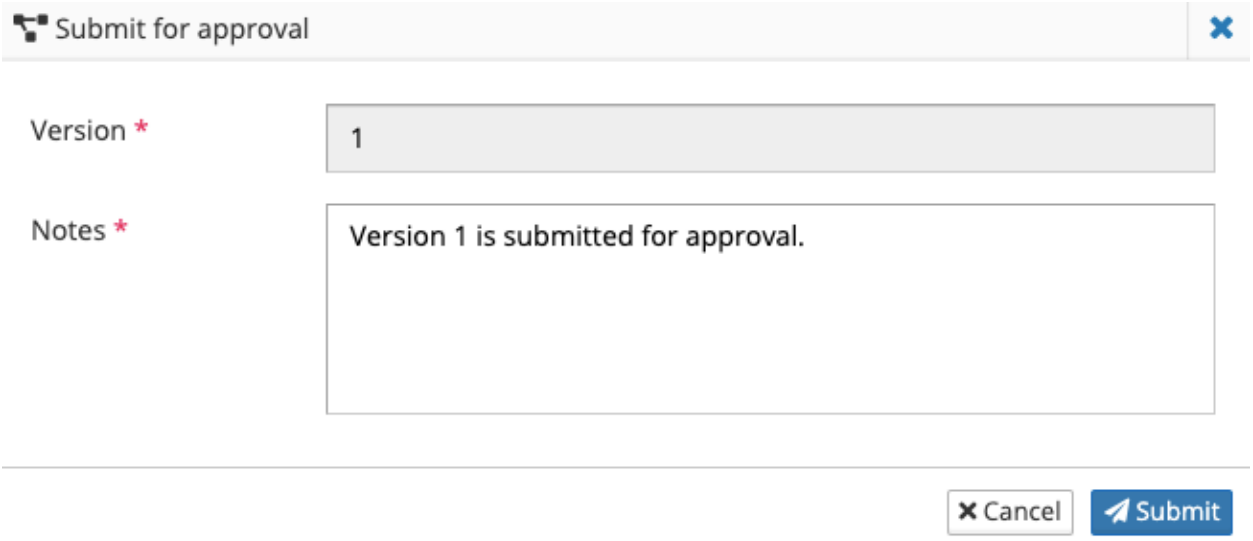


Example Excel Worksheet with Threats Output

	A	B	C	D	E
1		Threat	Source Name	Status	Risk
2	AWS CloudFront 2				
3		AWS - Insecure Communication	AWS CloudFront	Open	Very High
4		AWS - Insecure Interfaces and APIs	AWS CloudFront	Open	Very High
5	AWS EBS 3				
6		AWS - Confidential Data Exposure	AWS EBS	Open	Very High
7		AWS - Weak Identity, Credential and Access Management	AWS EBS	Open	Very High
8		AWS - Permanent Data Loss	AWS EBS	Open	Very High
9	AWS EC2 3				
10		AWS - Weak Identity, Credential and Access Management	AWS EC2	Open	Very High

Submit Threat Model for Approval

When you complete the Threat Model, click on “Submit for Approval.”

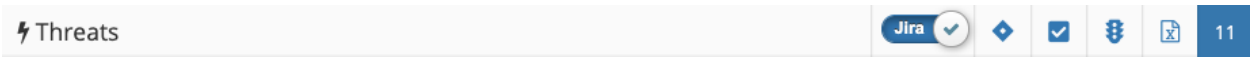


Your threat model is now complete. Since you have submitted it for approval it will be set to **Read only** mode. Your administrator will be notified via “Notifications” on the platform and it will show under Workflows. The threat model will remain in read only mode until it is returned for revisions. A red padlock  will be displayed next to the threat model name on the Diagram screen.

Working With Jira

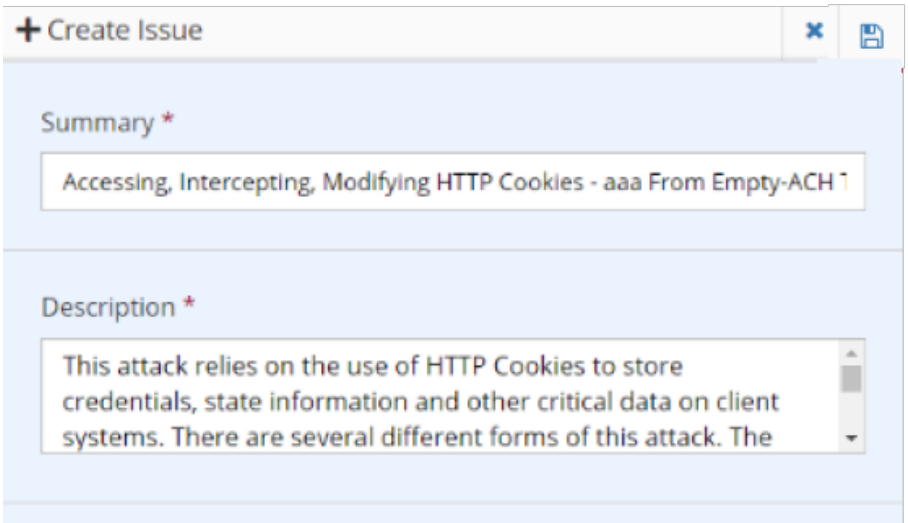
Opening a New Jira Ticket

1. Click on a threat in the Threats list. You can also click on a threat in the Security Requirements window.



2. Click on the  icon to create a new Jira issue within ThreatModeler.

Enter or modify the information to send to Jira.



3. Click Save. A new Issue is initiated in Jira. The threat in ThreatModeler now displays the Jira Issue ID.

Once You Create a Ticket in Jira, ThreatModeler's Bidirectional Integration Communicates Updates

- Anytime you make notes in ThreatModeler, they will appear as comments in Jira and vice versa.
- ThreatModeler updates the status for a Threat only when the JIRA issue is closed, by marking the item as Done. This status may vary for every organization.

Notifications

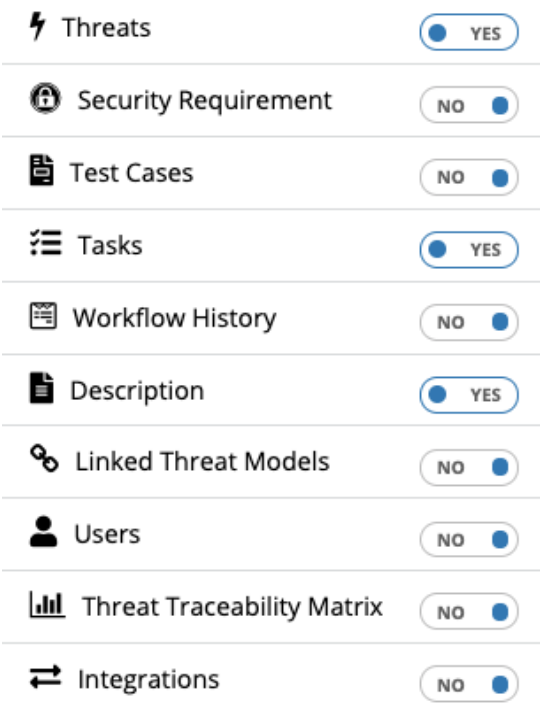
1. Cick on the  icon to access the Notifications popup window, which has three tabs.
   - **Notify** – displays version changes to your threat models, and users added or removed from your Groups.
   - **Workflow –** notifies you of threat models that have been submitted for your approval and threat models you have submitted for which you received an approval response.
   - **Task –** If you are mentioned in a task or have a comment in a task, you will receive a notification in the task tab.

2. Whenever you have new notifications, a red circle will appear over the notification icon showing the count of new notifications you have received.

Customizing Outputs on the Overview Screen

At any time, you can customize the output panels that are viewable on the Overview screen.

1. Click on the More  icon on the Overview screen to open a popup menu to place additional outputs onscreen. Once clicked, you will see a pull-down menu with all options that you can display (or not).
2. Click on each toggle button to select YES or NO. For example, if you want to display threats, toggle to YES.



Customization Options Summary

Threats

Shows a list and description of threats associated with your threat model.

Security Requirements

The Security Requirements panel is similar to the Threats panel, with Security Requirements grouped by source in a list with descriptions associated with your threat model.

Sample Arch for the cloud- 1

Source

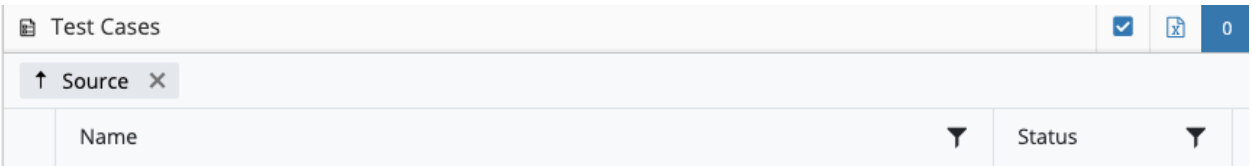
Security Requirement	Source Name	Status
AWS CloudFront		10
AWS - Configure CloudFront to return a custom error page when a request is blocked.	AWS CloudFront	Open
AWS - Disable origin identity	AWS CloudFront	Open
AWS - Enable API Authentication	AWS CloudFront	Open
AWS - Enable Access Logs	AWS CloudFront	Open
AWS - Encrypt Data At Rest	AWS CloudFront	Open
AWS - Encrypt data in transit	AWS CloudFront	Open
AWS - Ensure A Log Metric Filter And Alarm Exist For Unauthorized API Calls	AWS CloudFront	Open
AWS - Ensure logs generated by services are ingested in a bucket in the central logging account	AWS CloudFront	Open
AWS - Sign the restricted URL	AWS CloudFront	Open
AWS - Use AWS WAF to allow or block requests based on the rules in a web access control list	AWS CloudFront	Open

1. Sort or filter columns the same way. The status can be one of the following: Opened, Closed, Mitigated, Fixed, Not Applicable, Need More Details and Not Tested.
2. View the description for each item and add notes.
3. Click the arrow next to a component to open a list of Security Requirements associated with that component.

Test Cases

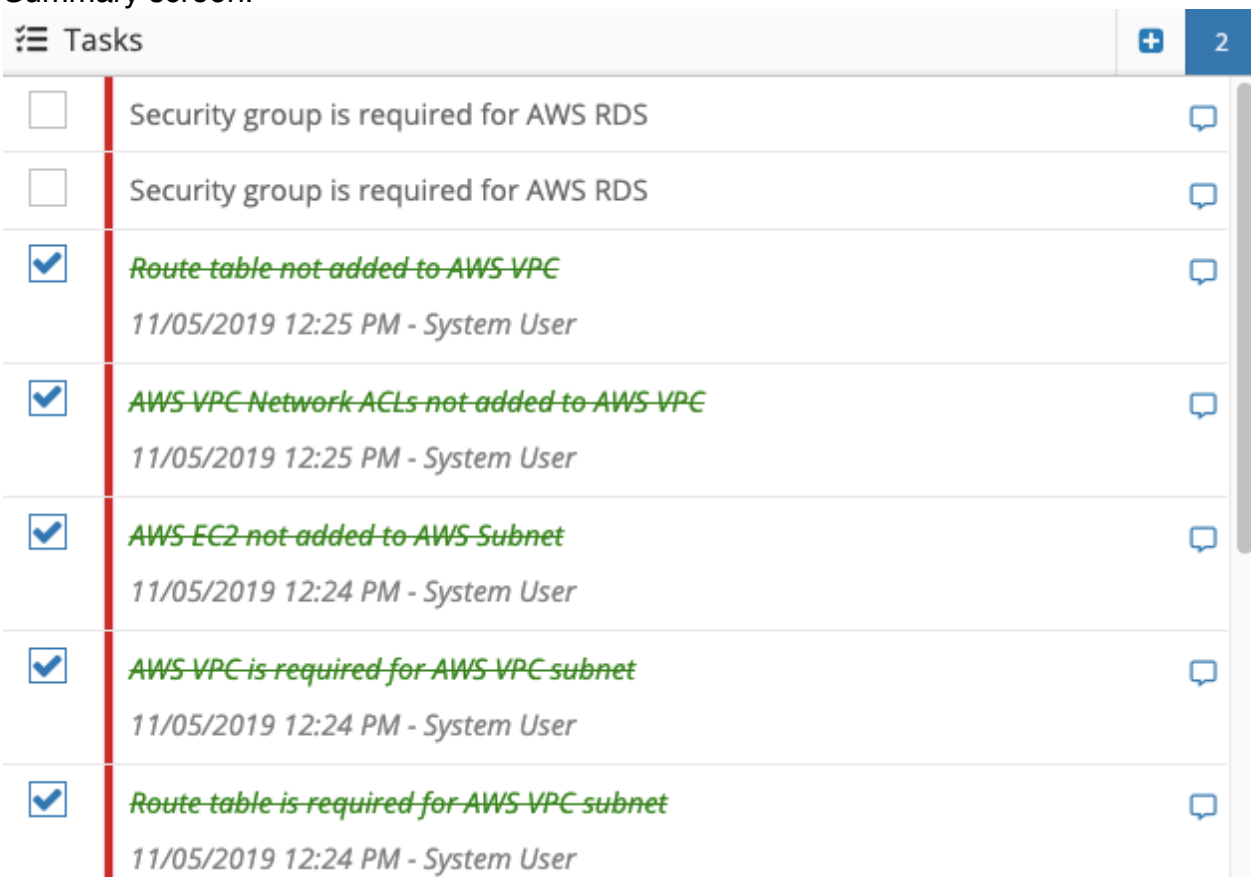
The Test Cases panel is similar to the Threats panel and is located under the Threats and Security Requirements Windows. It shows a list and description of the test cases associated with your threat model. By default, Test Cases are grouped by source.

- Sort or filter columns the same way
- View the description for each item and add notes.
- Change the status of a test case by clicking it and selecting the checkbox icon.



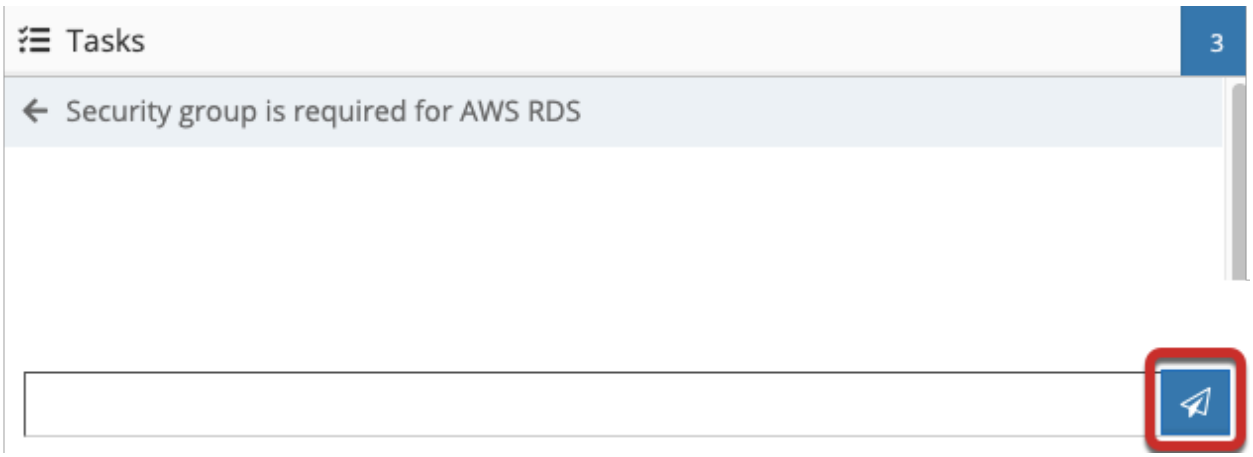
Tasks List

The Task List provides a list of tasks associated with your threat model. Adding and completing tasks will update the progress bar for that threat model on the Threat Model Summary screen.



1. Add more tasks using the  icon.

2. Provide a brief description of the action needed in the free text Define Task field.
3. Click the box next to a task to mark that task as complete.
4. Users can set the task urgency (High, Medium, Low)
5. Users can also input free text in the **Explain Task** field.
6. As in the other Tasks field, users can click on a task to add and review comments in a free text field, then click Send.



Workflow History

The Workflow History shows the approval workflow for a threat model.

Description

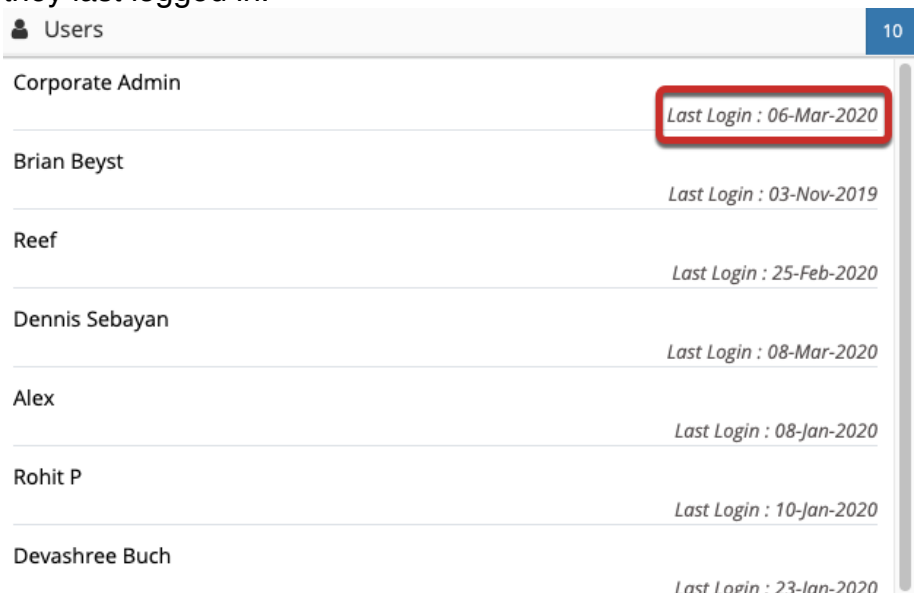
The Description shows the Summary text for your model, generated when you created it. Click on the edit icon in the top right corner to make changes. The Description will show up on the Report.

Linked Threat Models

The Linked Threat Model panel shows a list of all the threat models linked with a particular threat model. When you nest the current threat model into another threat model, the list of all threat models will be provided here, and so on.

Users

Shows a list of all the users that have permission to access this threat model, and when they last logged in.



Threat Traceability Matrix

Shows a Threat Traceability Matrix for this model – a graphical view of the associated threats grouped by status and risk level. In the Overview screen, you can toggle between the bar graph and chart by risk status views.

Nesting and Chaining Threat Models

Whenever you create a threat model, it is added to your Toolbox as a full component. If you created a threat model – for example a bill pay system – you can add it to subsequent models. Sometime referred to as “chaining,” nesting is a process of incorporating an active threat model into another threat model, treated as a component from the Diagram screen Toolbox.

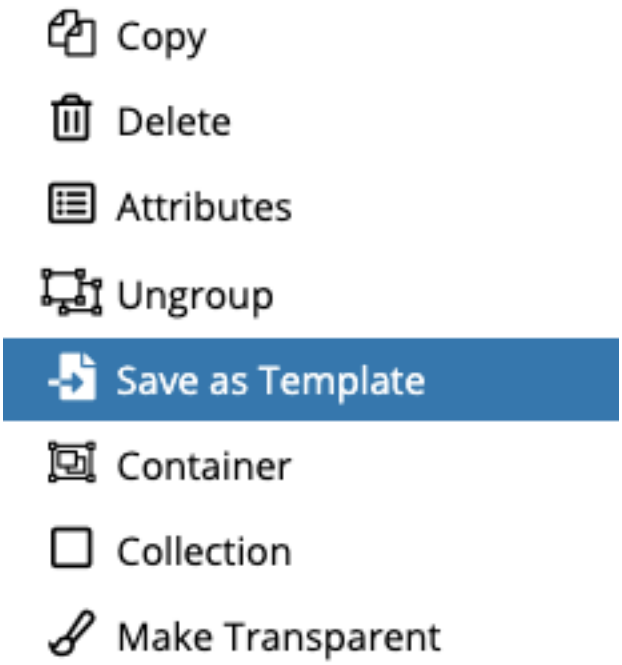
ThreatModeler does not limit the number of nested threat models or the depth to which threat models may be nested. Nesting allows the inserted threat model to become a component of another threat model. Users have the option of adding the nested threat

model's threats into the receiving threat model. When you make an update to one threat model, all associated threat models are automatically updated.

Creating a Template from a Partial Threat Model

You can keep just a portion of the canvas contents as a Template.

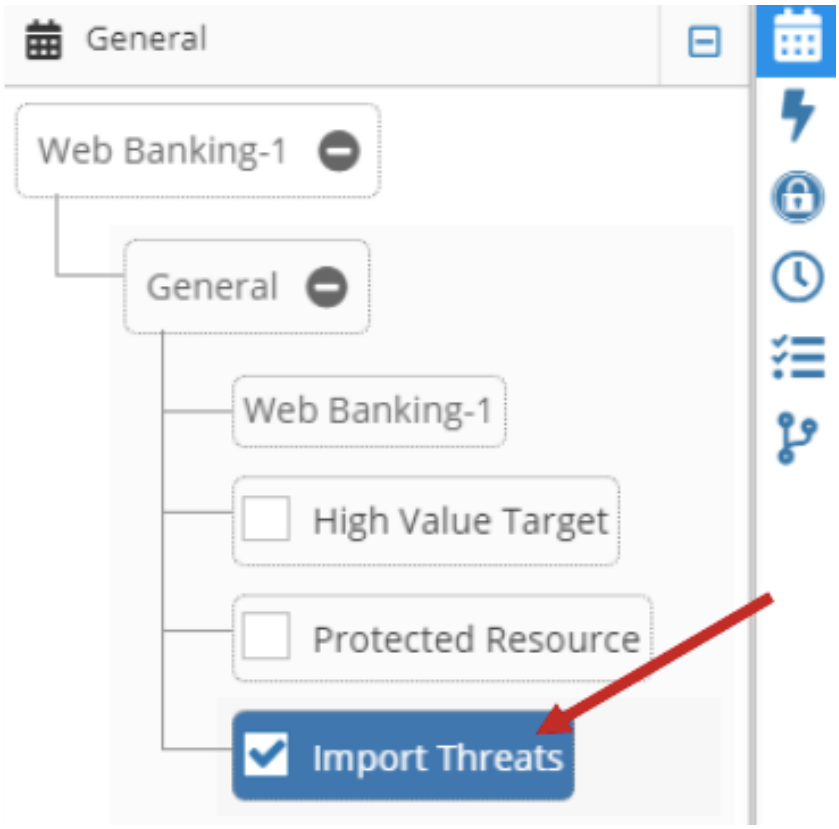
1. Right-click on the Group that you'd like to turn into a Template.
2. Select the desired components either by using the SHIFT + Click; or Ctrl + Click keys, or by dragging a box.
3. Click on the Group button on the Diagram Toolbar.
4. Right-click the Group to access a pop-up options menu.
5. Choose Save as Template.



Importing Threats to a Larger Threat Model

The advantage to using a threat model instead of a generic component is that you can import the threats from one threat model component into your larger model.

1. Select the nested threat model component.
2. Open the General Properties window.
3. Click "Import Threats." The number of threats identified in your model should increase.



Working with Templates

Templates are baseline architectures. saved from the diagramming canvas into the Template's Library. Templates are not active threat models, but reusable building blocks to build upon. The saved Templates can include any variety of:

- Components
- Communication protocol links
- Component properties
- Groups

Using the Template Builder

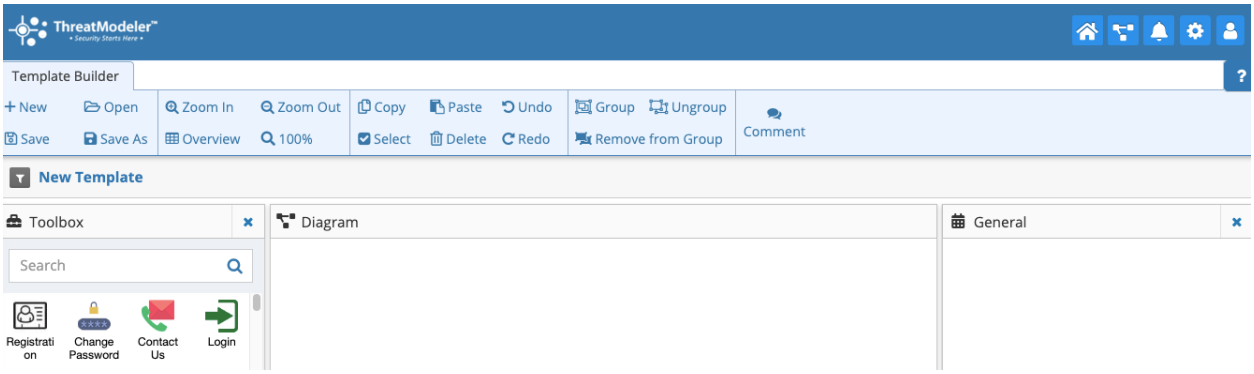
Stored Templates do not generate outputs until they are utilized within a threat model. As such, Templates do not consume ThreatModeler licenses. A convenient functionality behind this is that your two threat models (the smaller one that you are using as a component, and the larger one in which it is placed) are now chained together.

Changes and updates that you make to the component threat model, e.g., upgrades to the bill payment system, will automatically reflect in the corresponding component form of any threat model in which it is placed.

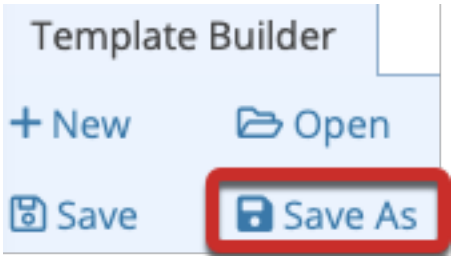
Template Builder Method One

1. Click on the 

icon from the Settings 
drop-down menu. ThreatModeler will navigate to the Template web page, which is similar to the threat model Diagram screen.

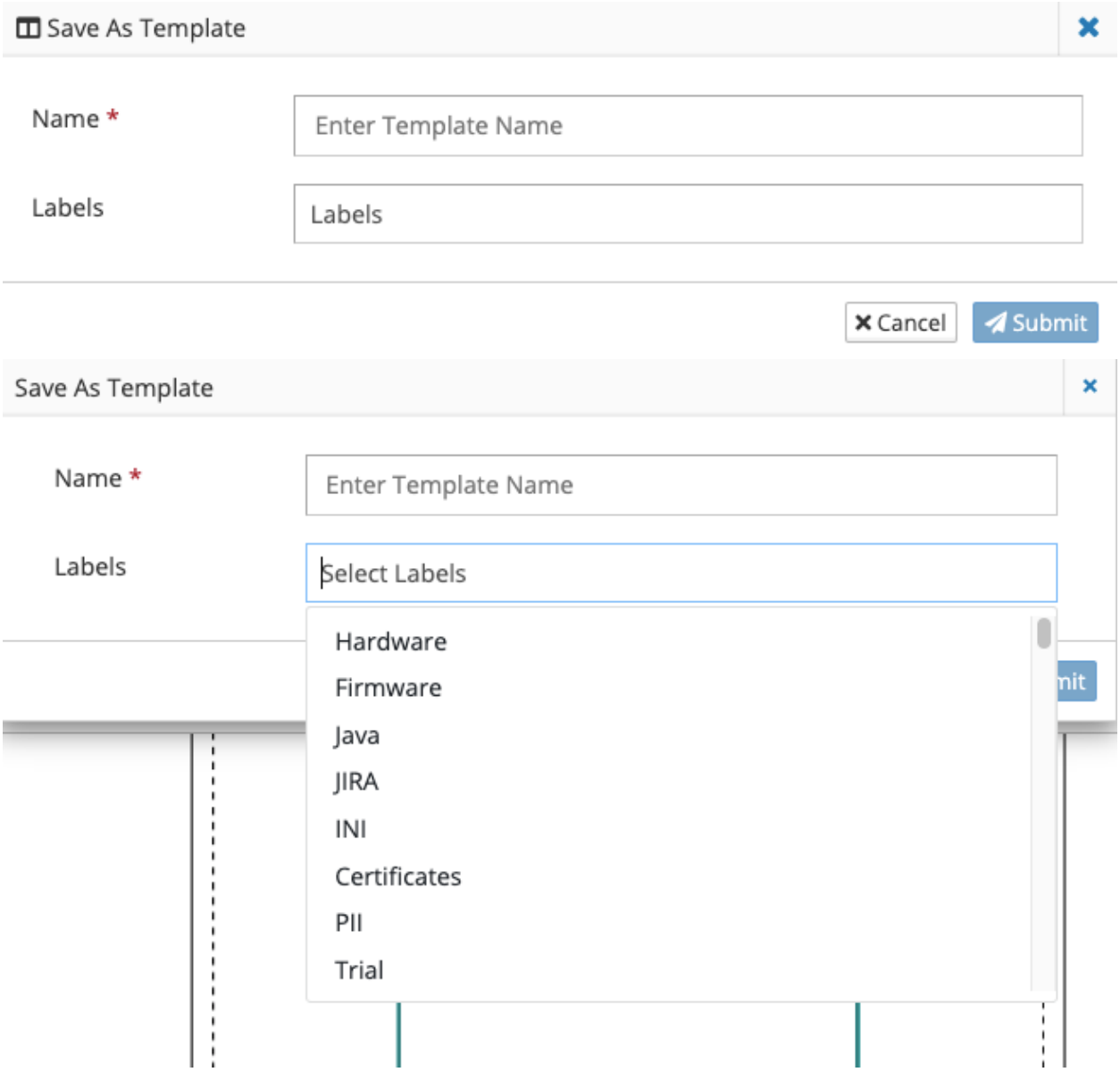


2. Create the diagram.
3. Click the Save button on the top left.



Template Builder Method Two

6. Open an existing threat model.
7. In the Diagram canvas, update the diagram.
8. Click on the More  icon.
9. Select Save ThreatModel as Template. The Save Diagram as Template dialog box pops up.



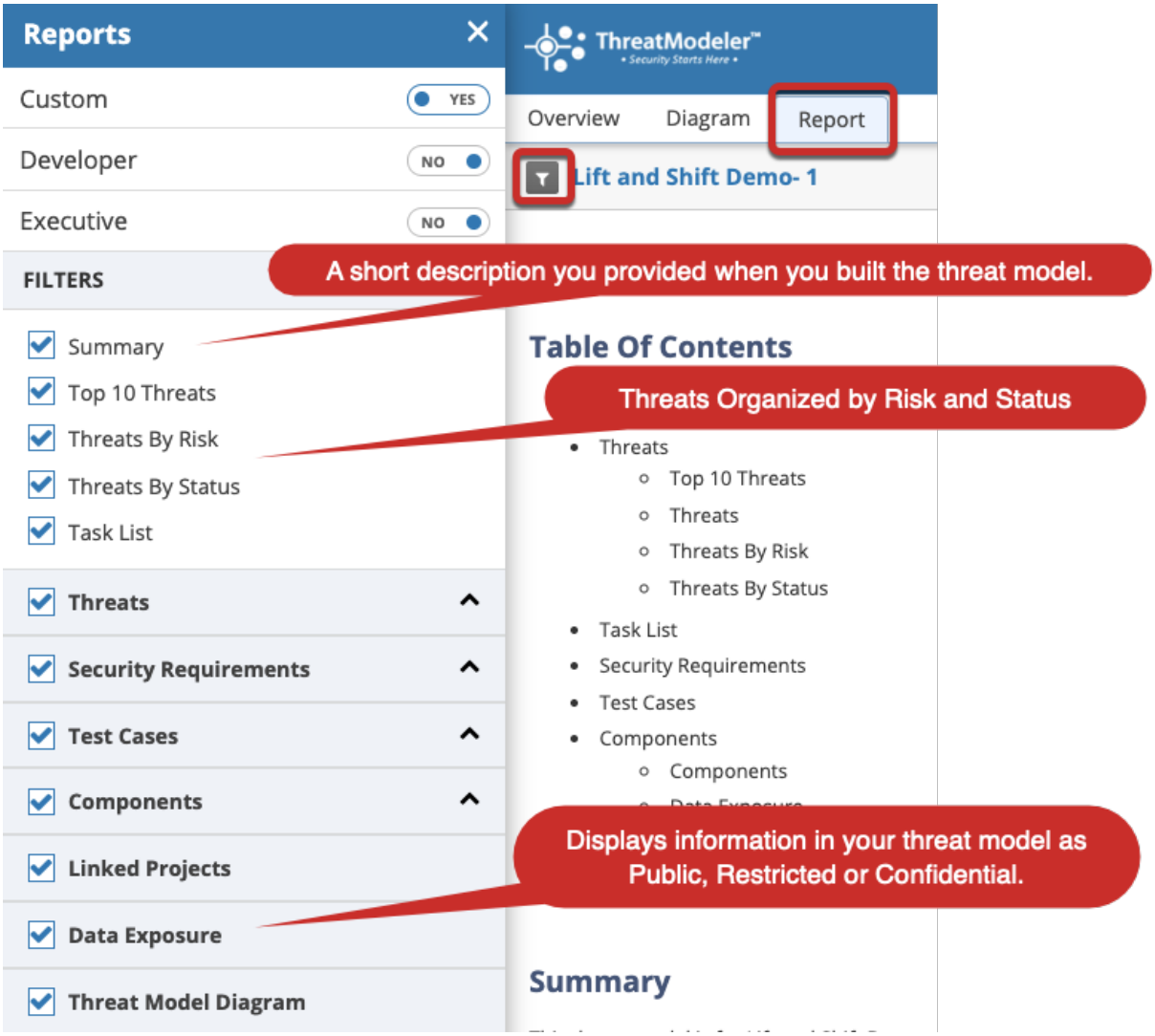
10. Add the Template Name and select one or more labels and click Submit.

Working With Reports

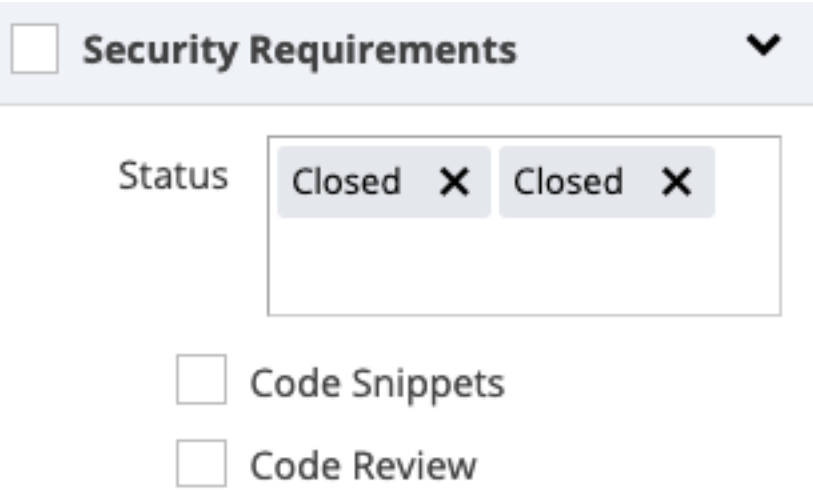
Clicking the Report tab will take you to the Report screen with a current report of your threat model. Click on the filter  icon above the report, which opens the Filter slider to customize reports. The report is customizable and can include the following details:

- Summary – a short description you provided when you built your model.

- Threats – includes the Top 10 Threats, and threats organized by Risk and Status.
- Task List – displays items that were not addressed.
- Threats Detail – four lists with a detailed summary, which includes:
    - Threats identified by your model.



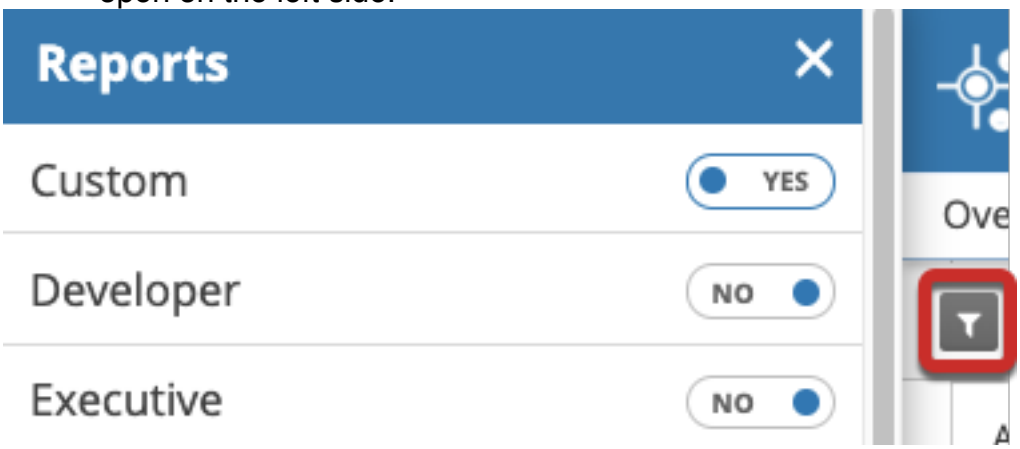
    - Security Requirements associated to threats.



- Test Cases.
- Threat Model Components.
- Linked Projects – a section that lists any projects that are linked to that threat model.
- Data Exposure – a data classification chart for ease of understanding.
- Full Threat Model – the diagram will be at the bottom of the report.

Customizing your Report

1. On the Report screen, click on the Filter  icon. A sliding panel will slide open on the left side.



2. Select report recipient. Based on your role, you will have access to certain information. Selecting a Report user type will automatically negate all other report types.

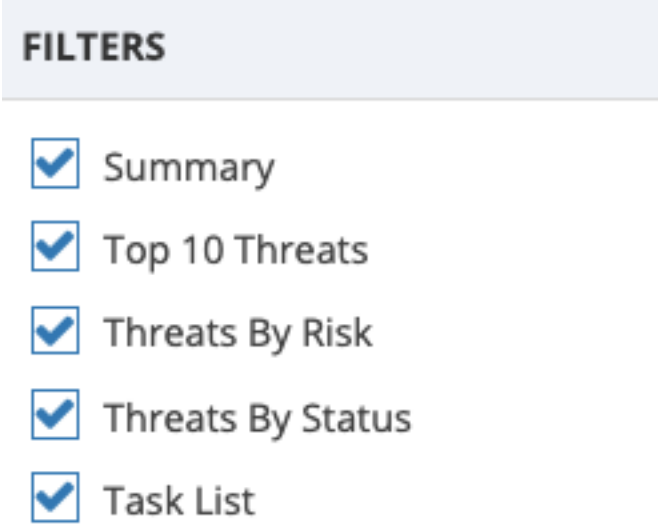
Three Main Report Types

Custom – displays everything from all the Report tabs. This is the most comprehensive Report and includes the Summary, Threats (in multiple views), Task List, Security Requirements, Test Cases, Components (including Data Exposure and Linked Projects) and the ThreatModeler Diagram. To create a Custom Report:

1. Click “Custom Report.”
2. Select or deselect components from sections in the filter list.

Developer – suitable for a person who builds, debugs and deploys software. It will display Threats, Security Requirements and Test Cases.
Executive – appropriate for a person who oversees application development and other technical operations. It will display a Summary, Top 10 Threats, Data Exposure and Linked Projects.

Filtering Reports

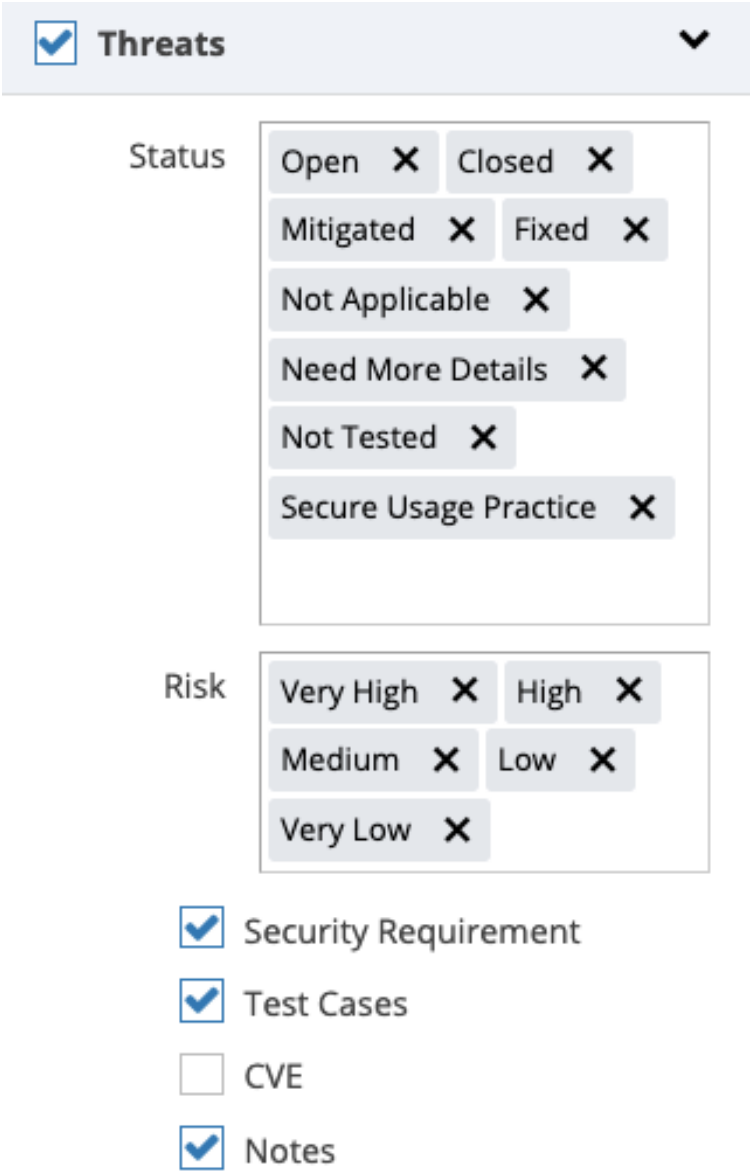


Users can select pre-defined filters or define their own. Different filters may be selected from the drop-down menu at the top of the Filter slider.

Filtering Threats

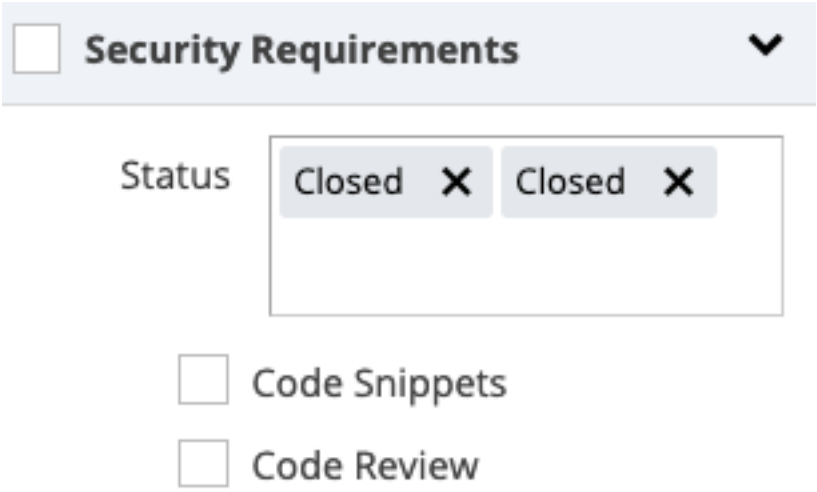
Select the threats to include in the report based on status and risk rating. The Threats section of the report also includes Security Requirements, Test Cases, CVE IDs and Notes for identified threats.

At a threat level, users can view the description of a specific threat, add their own notes, and change the status and risk level. For Security Requirements and Test Cases, since there is no risk rating associated, users will only be able to add notes and change the status.



Filtering Security Requirements

Select the mitigating requirements and test cases to show. As with threats, Security Requirements are included by adding desired statuses to the filter. Each Security Requirement also provides, when applicable, associated code snippets and code reviews.



Appendix

ThreatModeler AWS Accelerator Setup

A. IAM Role (Skip this step if you are not self-hosting ThreatModeler)

1. Login to AWS console
2. Navigate to IAM
3. Click on Roles and then select “Create Role”
4. In the first step of the wizard select EC2, Click Next
5. Now select policy “ReadOnlyAccess”
6. Add the tags (Optional)
7. Please add a Name for the role “ThreatModeler”.
8. Navigate to EC2 and click EC2 dashboard
9. Select the EC2 instance hosting ThreatModeler
10. Associate IAM role “ThreatModeler” to the EC2 instance hosting ThreatModeler
11. Pre-requisite – AWS Config has to be enabled

B. IAM User

1. Login to AWS console
2. Navigate to IAM
3. Click on Users and then select “Add User”
4. Please Enter user name “ThreatModeler” and select programmatic access.
5. Click Next, now select attach existing policy and add “ReadOnlyAccess” policy to the user

6. Add the tags (Optional)
7. Create the user.
8. Copy the access key and secret Key of the User.
9. Login into ThreatModeler
10. Navigate to Third-party integrations using the settings  Icon
11. On the instances panel click on Add instance and select AWS
12. Provide a friendly Name
13. Enter the Access & Secret Key and click save.
14. ThreatModeler AWS Accelerator Setup
15. Pre-requisite – AWS Config has to be enabled

Additional Resources

To learn more about threat modeling and ThreatModeler Software, Inc., visit our webpage at www.threatmodeler.com.

To get additional support or to discuss your specific threat modeling needs, contact support@threatmodeler.com.

Visit our YouTube page to view threat modeling videos in a variety of cyber systems.