2020

ThreatModeler
SECURITY STARTS HERE

ThreatModeler™: Threat Modeling Scenarios for AWS

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

Table of Contents

Overview

As more organizations embark on the journey to the cloud, taking appropriate measures to build security within the design phase is crucial – from the perspective of data protection, identity and access management, incidence response, resilience and overall infrastructure security. Threat modeling has emerged as a necessary activity to implement security and identify security gaps early on. The purview of threat modeling falls under two broad categories:

Category 1: New Applications
This category covers all scenarios involving new and/or fresh developments on AWS.

Category 2: Existing Applications
The journey to the cloud often starts with deploying applications in Dev/Test environments before moving them into a production environment

For both scenarios, threat modeling needs to be seen as an integrated activity that allows you to view the relevant security configurations. This helps any organization to make security decisions and build cloud environments securely.

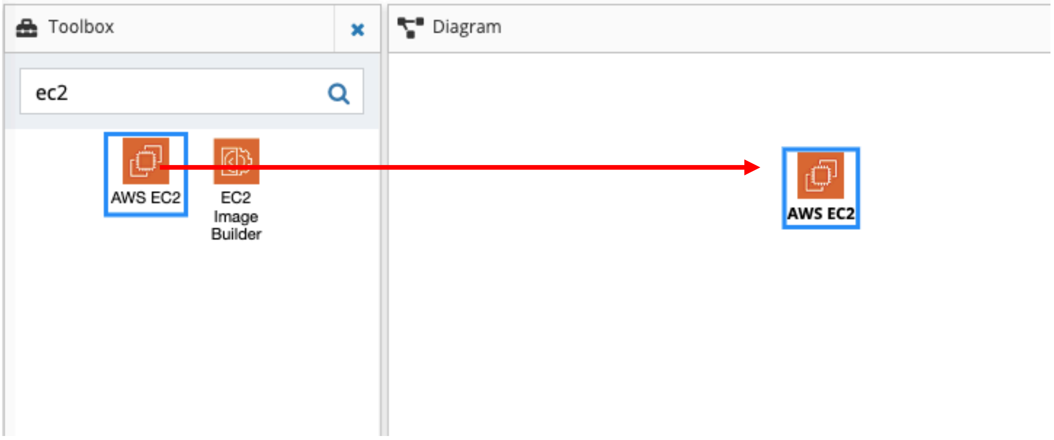
Scenario 1 – User Developing a New Application on AWS

In this scenario, the user is building a new application on AWS. To identify and prioritize security capabilities that must be built in, they must build a threat model. Given the pace of innovation at AWS (with frequent releases of new services and features) this user might have limited knowledge on the security capabilities that the AWS services provide and the dependencies to configure them securely.

ThreatModeler Assist provides the user with steps to complete the threat model diagram and identify dependencies.

Building a Threat Model From Scratch Using ThreatModeler Assist

1. Create a new threat model.
2. Begin placing items on the Diagram screen canvas, e.g. place an EC2 component. ThreatModeler Assist conducts the automated analysis.

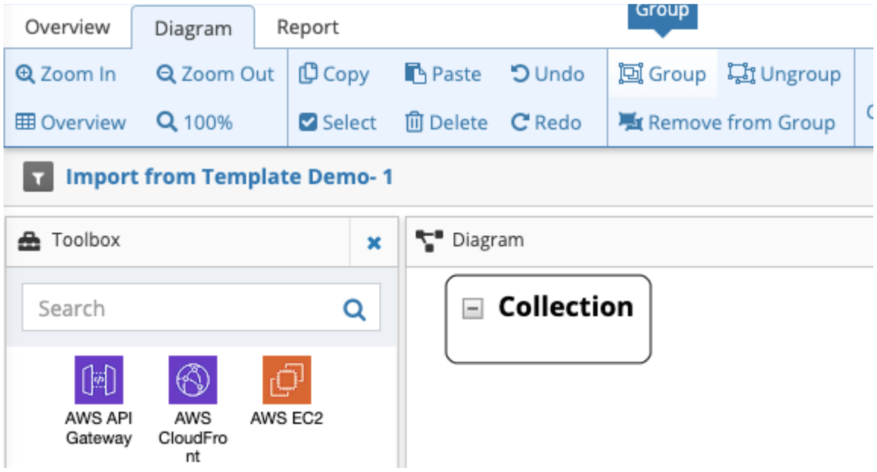


Optional – Change Component Representation

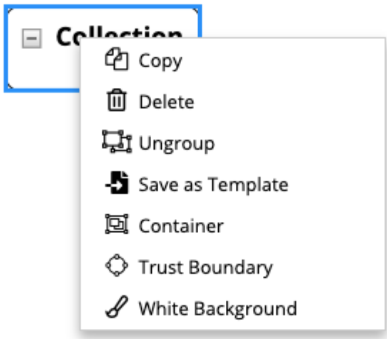
Representation of any component is key when building a diagram. In this example, you can choose to show EC2 as a container instead of a stand-alone component to further represent any underlying applications within.

To do so:

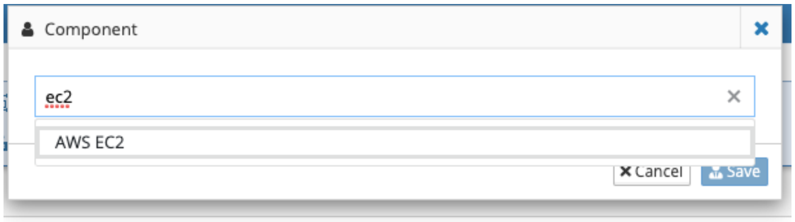
1. Click once on the empty canvas.
2. Navigate to the toolbar on the top and click on “Group.” This will create a collection box on the diagram.

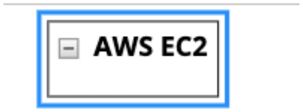


3. Right click on the text of the Collection box and select “Container.”

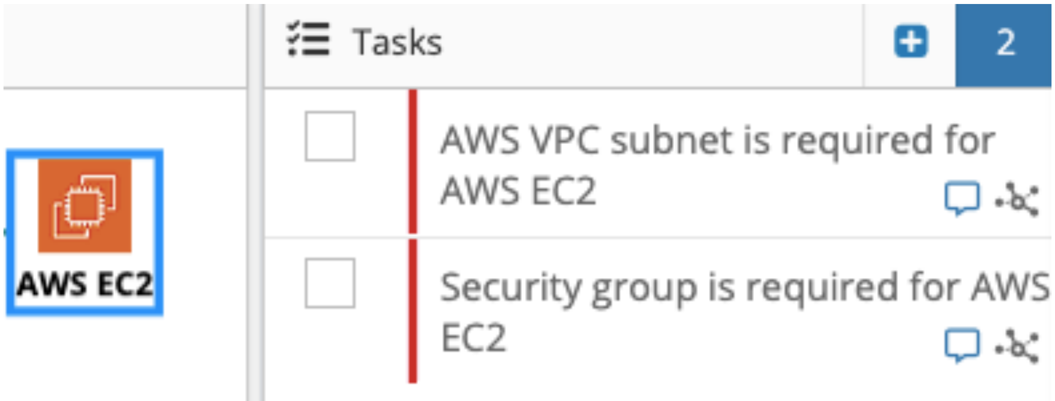


4. From the pop-up menu, type the name of the service/component you wish to select, for e.g., EC2. Hit Save. This will create a container that represents EC2 and carries the same properties as if the component was brought in as a standalone icon.





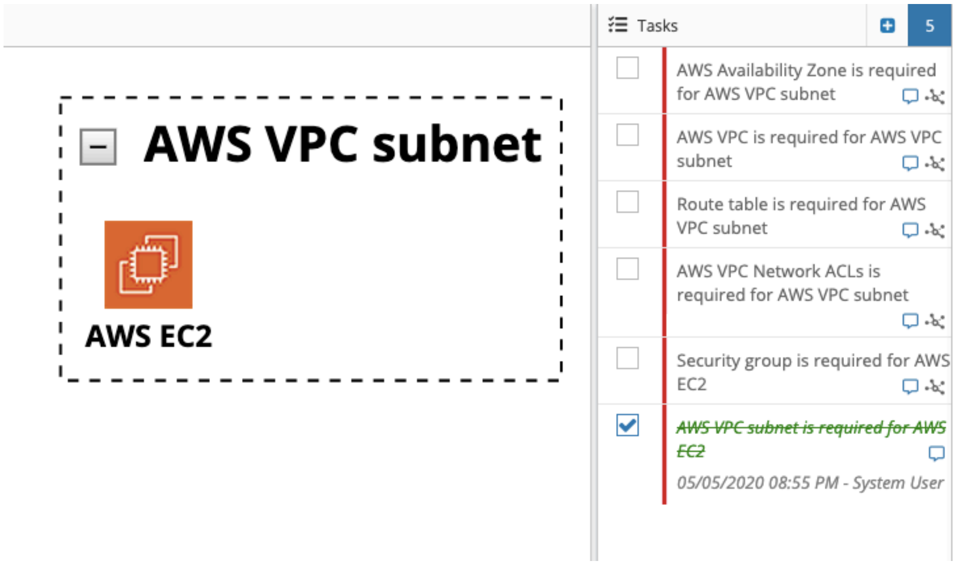
5. ThreatModeler creates open tasks for items that need to be accomplished in order to complete the architecture around the component. These tasks are in-line with the established rules.



□ AWS VPC subnet is required for AWS EC2

□ Security group is required for AWS EC2

6. As tasks are executed for the threat model, they will be checked as completed in the task list. New tasks may be added to the threat model based on any new dependencies.



□ AWS Availability Zone is required for AWS VPC subnet

□ AWS VPC is required for AWS VPC subnet

□ Route table is required for AWS VPC subnet

□ AWS VPC Network ACLs is required for AWS VPC subnet

□ Security group is required for AWS EC2

☑ ~~AWS VPC subnet is required for AWS EC2~~
05/05/2020 08:55 PM - System User

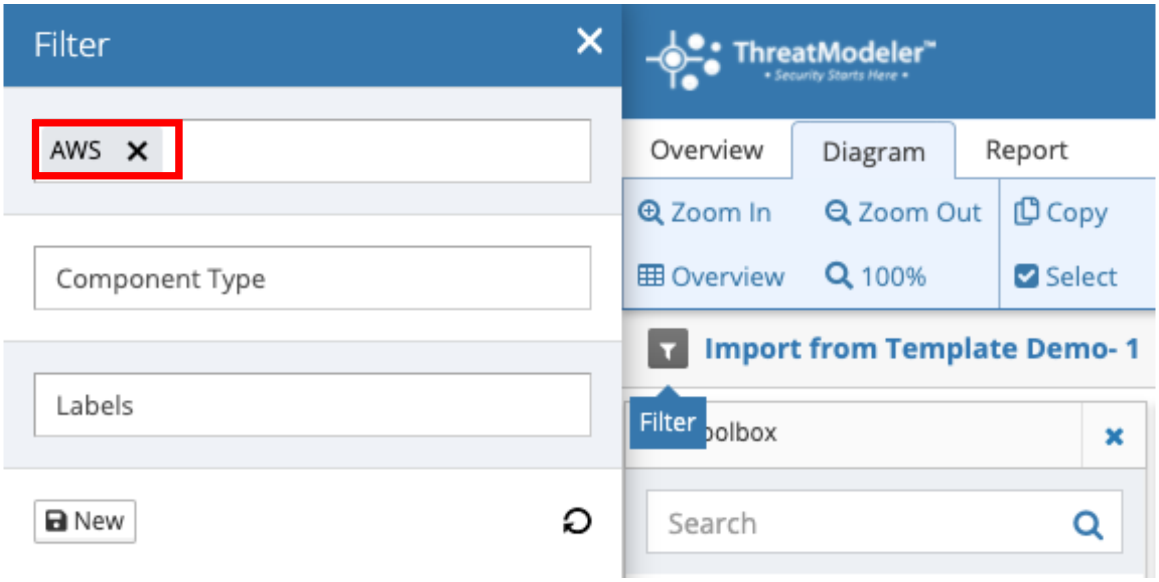
Scenario 2 – Associating Application and Infrastructure Threat Models

For a complete overview of the security posture of the application's stack across all layers, threat models developed by application developers and application security must be associated with the threat models developed for the infrastructure.

Nesting of Threat Models

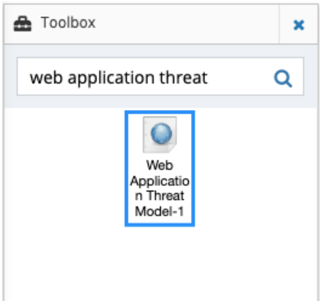
Once your infrastructure layer is identified using Assist, it's now time to view the full-stack architecture by bringing in a threat model for the application that resides within the workload. To do so:

1. Navigate to the filters for the toolbox and ensure that all filters have been removed.



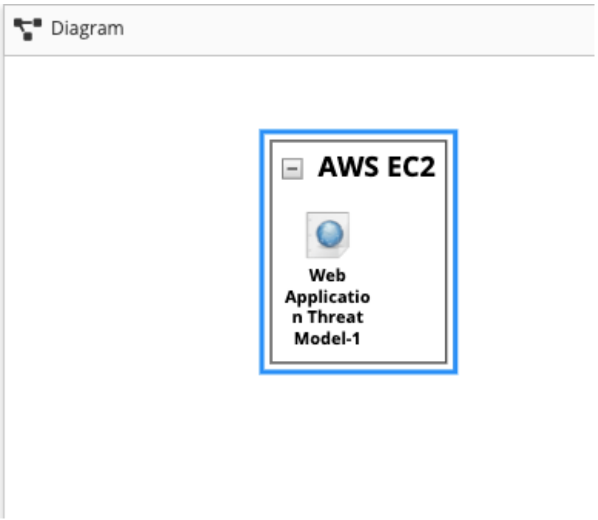
If a filter exists, click on the "x" right next to the name to remove.

2. From the toolbox, search for the threat model of the application you would like to use within this architecture.

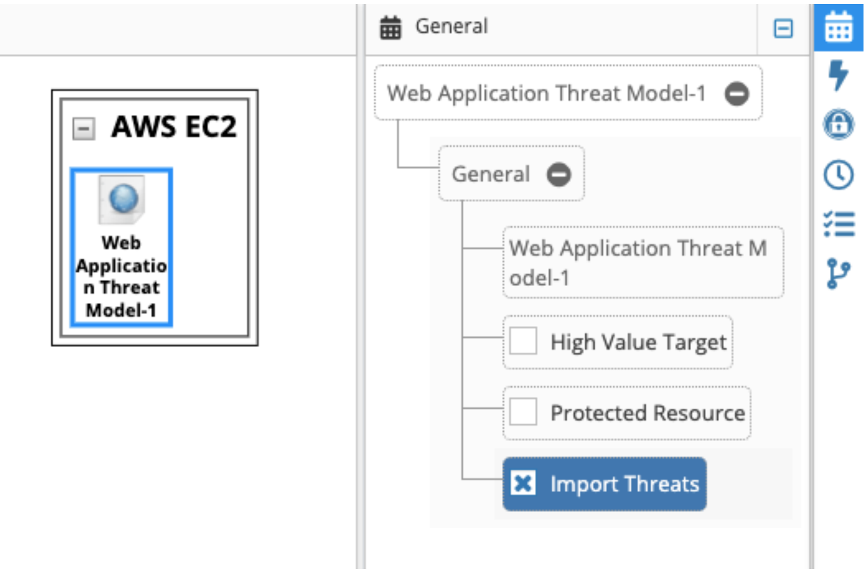


Each threat model built in ThreatModeler can be used as a component in any other threat model within the portfolio.

3. Drag and drop the threat model component on the canvas.



4. With the component selected, navigate to the General Properties, and select "Import Threats."


AWS EC2
Web Application Threat Model-1
General
Web Application Threat Model-1
General
Web Application Threat Model-1
□ High Value Target
□ Protected Resource
Import Threats

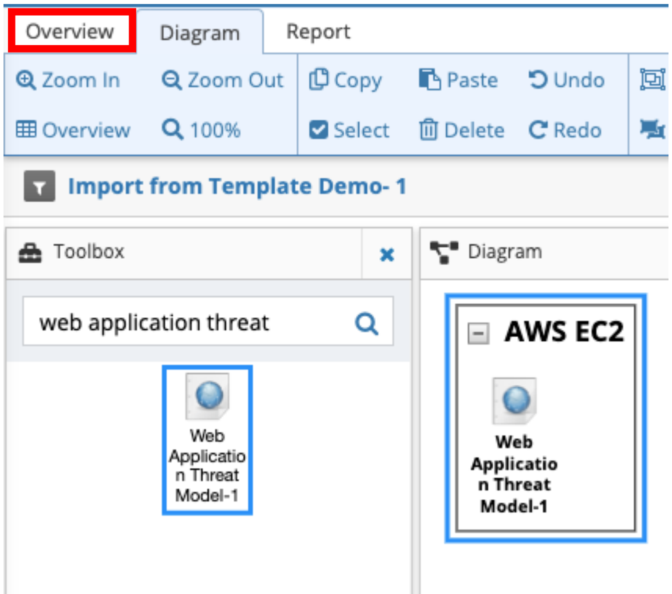
Scenario 3 – User Wants to Analyze and Report on Their Security Posture

After the user has developed a threat model and defined attributes for the components, they will want to review, analyze and report on specific security findings to address any gaps or prioritize roadmap items as part of their security objectives.

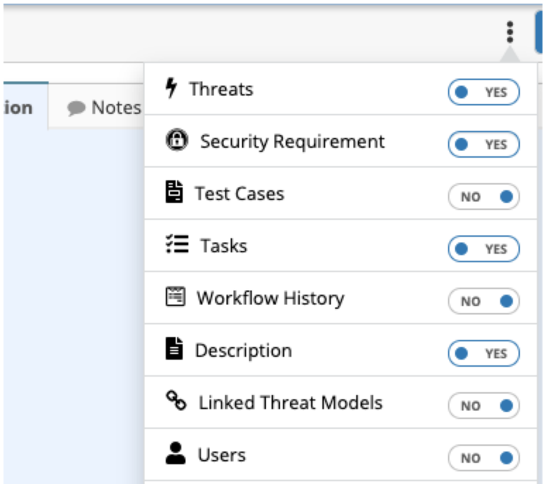
Threat Analysis and Management

To review the findings from a threat model:

1. Navigate to the Overview screen.

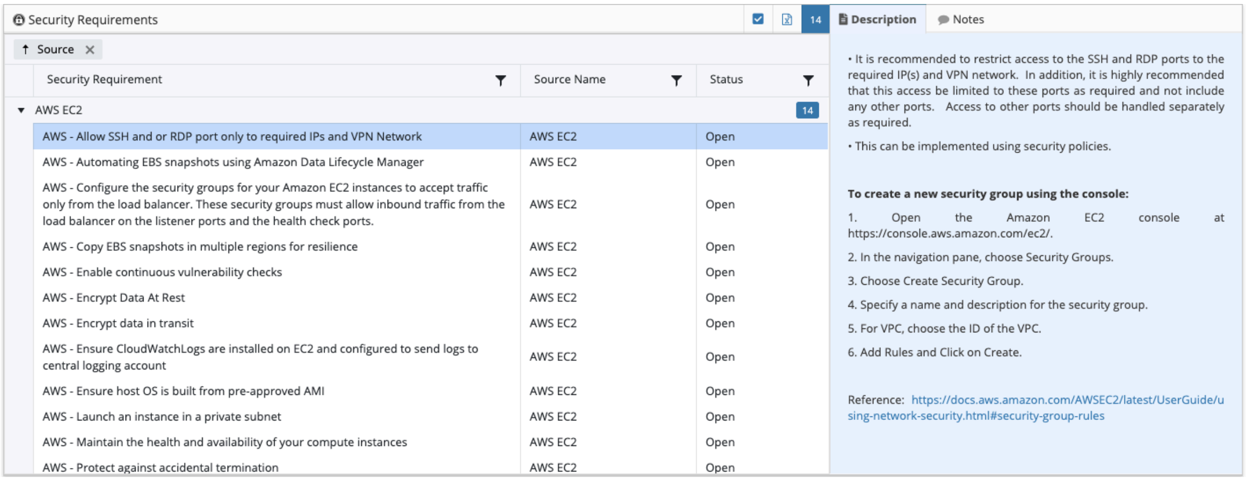


2. Click on the ⋮ icon and ensure that Security Requirement is marked as "Yes."



Threats YES
Security Requirement YES
Test Cases NO
Tasks YES
Workflow History NO
Description YES
Linked Threat Models NO
Users NO

3. In the Security Requirements pane, you will be able to view all the controls required for you to implement.



Security Requirement	Source Name	Status
▾ AWS EC2 14		
AWS - Allow SSH and or RDP port only to required IPs and VPN Network	AWS EC2	Open
AWS - Automating EBS snapshots using Amazon Data Lifecycle Manager	AWS EC2	Open
AWS - Configure the security groups for your Amazon EC2 instances to accept traffic only from the load balancer. These security groups must allow inbound traffic from the load balancer on the listener ports and the health check ports.	AWS EC2	Open
AWS - Copy EBS snapshots in multiple regions for resilience	AWS EC2	Open
AWS - Enable continuous vulnerability checks	AWS EC2	Open
AWS - Encrypt Data At Rest	AWS EC2	Open
AWS - Encrypt data in transit	AWS EC2	Open
AWS - Ensure CloudWatchLogs are installed on EC2 and configured to send logs to central logging account	AWS EC2	Open
AWS - Ensure host OS is built from pre-approved AMI	AWS EC2	Open
AWS - Launch an instance in a private subnet	AWS EC2	Open
AWS - Maintain the health and availability of your compute instances	AWS EC2	Open
AWS - Protect against accidental termination	AWS EC2	Open

• It is recommended to restrict access to the SSH and RDP ports to the required IP(s) and VPN network. In addition, it is highly recommended that this access be limited to these ports as required and not include any other ports. Access to other ports should be handled separately as required.

• This can be implemented using security policies.

To create a new security group using the console:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

2. In the navigation pane, choose Security Groups.

3. Choose Create Security Group.

4. Specify a name and description for the security group.

5. For VPC, choose the ID of the VPC.

6. Add Rules and Click on Create.

Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#security-group-rules

These security requirements provide detailed guidance around implementation of the Security Epics (IAM, Data Protection, Incidence Response, Resilience and Infrastructure Security).

Scenario 4 – User Wants to Create a Repeatable and Reusable Threat Modeling Process

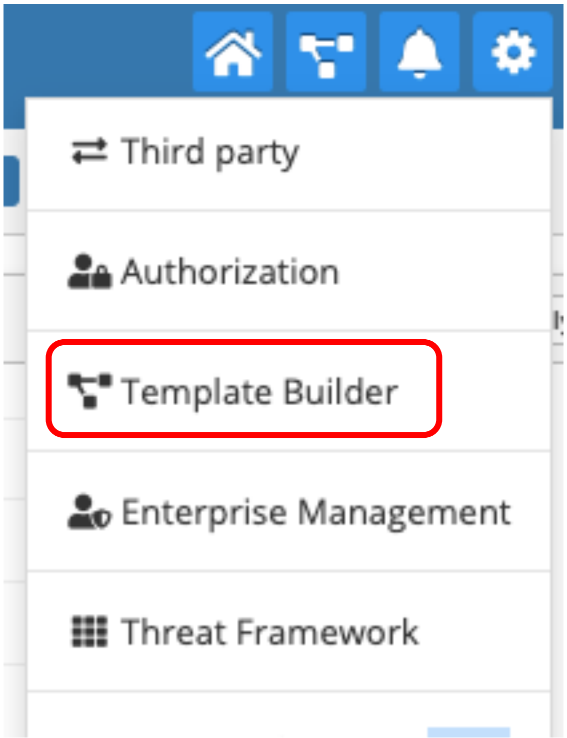
Once a design pattern is approved, a user should be able to reuse such designs for future deployments. This will allow the user to build standardization into their AWS deployments.

Templates are reusable design patterns that can be leveraged to kickstart the threat modeling activity when moving workloads and applications into AWS.

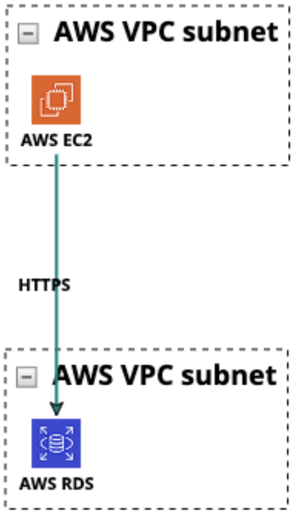
Building a Template From Scratch

Before you begin, make sure that you have access to the Template Management section of ThreatModeler. Reach out to your ThreatModeler Admin for access provisioning.

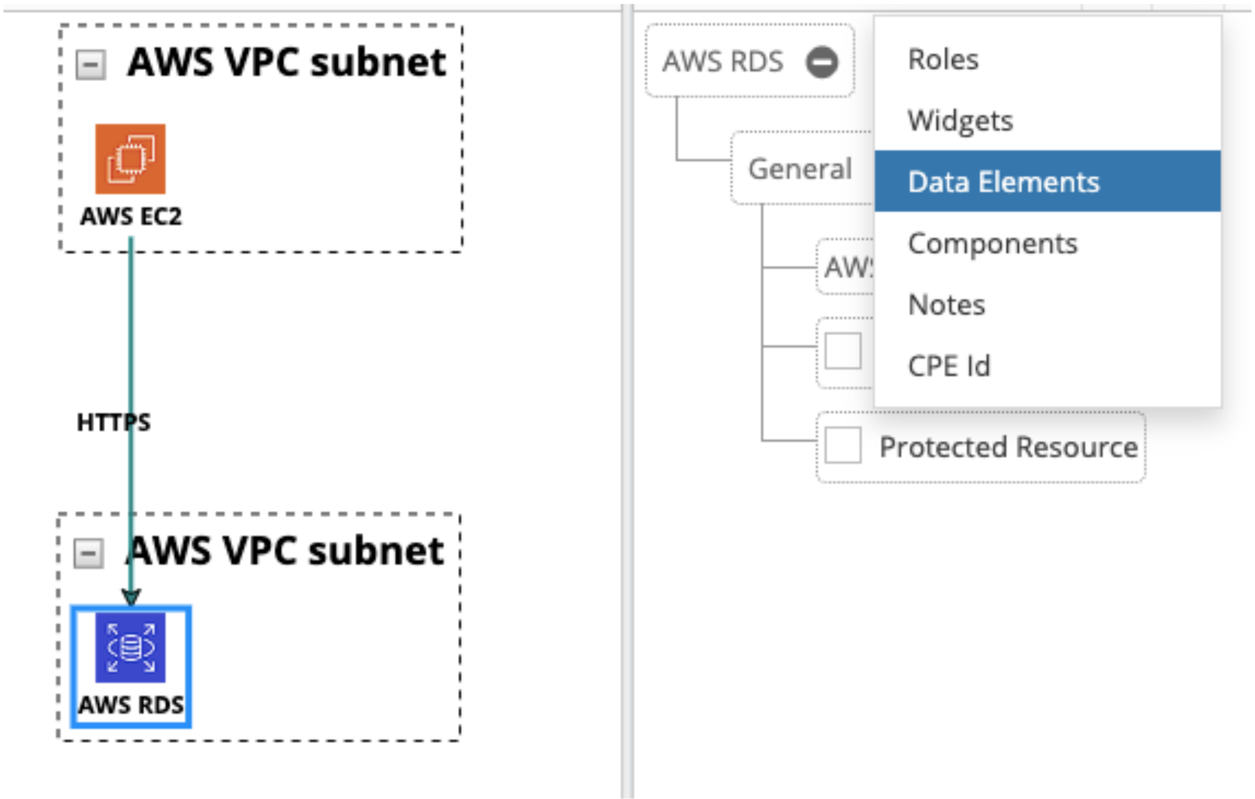
1. Navigate to Template Builder from Settings.



2. Build a diagram of the standardized architecture by dragging and dropping components and protocols.



3. Associate any properties to the components (e.g. Data Elements on the RDS).



4. Click Save As, input a template Name. Click Submit.

Create a Template from a Pre-Existing Threat Model

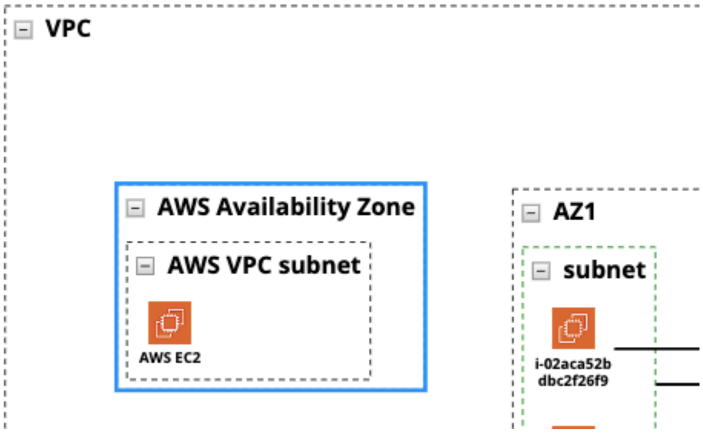
Alternatively, you can create a template directly from a pre-existing threat model. To do so:

1. Open a threat model from which you would like to create a template.
2. Navigate to the ⋮ icon on the diagram screen.
3. Select Save Threat Model as Template.
4. Input a template Name and click Submit.

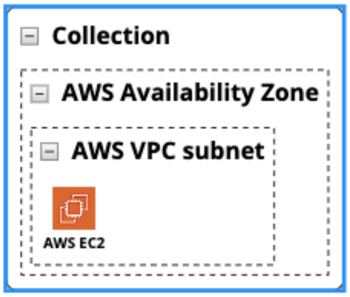
Saving Partial Threat Model Components as Templates

When creating a template from a threat model, you also have the option of saving partial threat model components as part of the template. To do so:

1. Open a threat model from which you would like to create a template.
2. On the diagram, select the architectural components from which you would like to create a template.



3. From the Toolbar on the top, Click the “Group” icon.

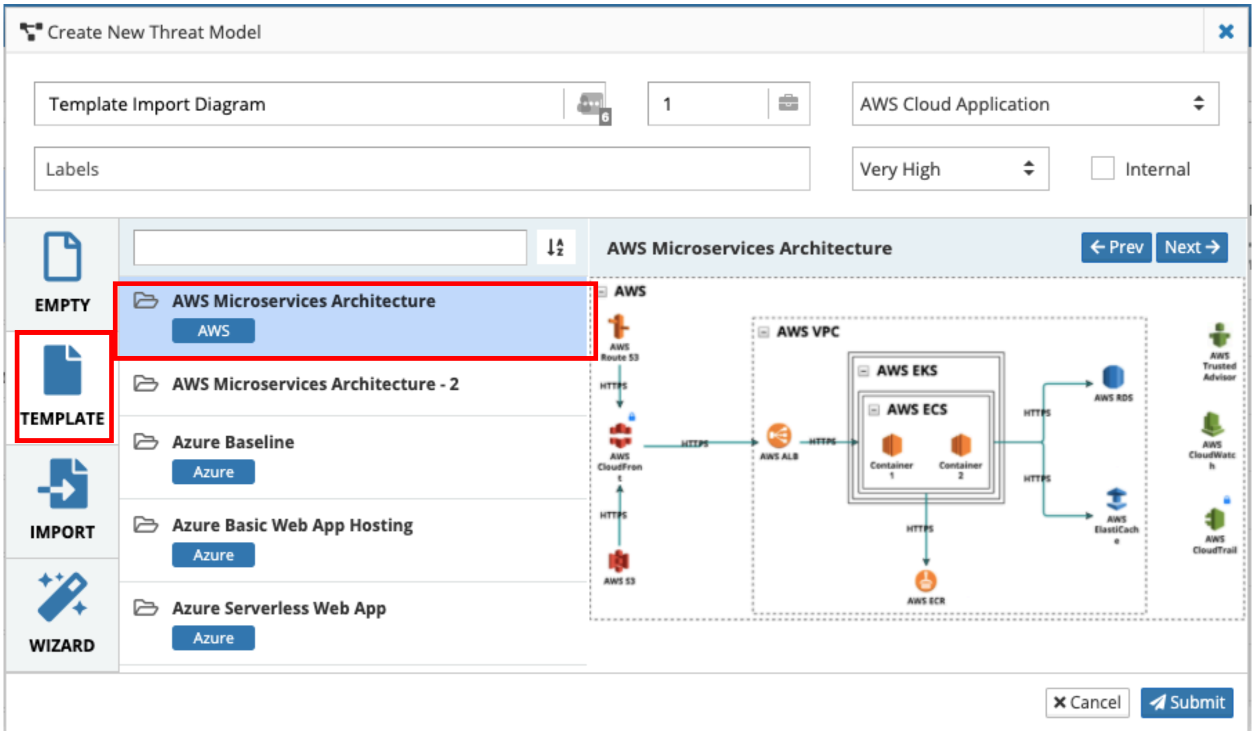


4. With the Group selected, navigate to the ⋮ icon on the diagram screen.
5. Select “Save Group as Template.”
6. Input the template Name. Click Submit.

Using Templates to Build Threat Models

When you start to build a threat model, you have the option to use pre-built design patterns as a way to kickstart your threat modeling activity. To do so:

1. Click the ➕ icon on the Threat Models page.
2. Provide basic details about the threat model (Name, Version, Project Type).
3. On the left side menu options, select the Template option.



Create New Threat Model

Template Import Diagram | 1 | AWS Cloud Application

Labels | Very High | □ Internal

EMPTY
TEMPLATE
IMPORT
WIZARD

- AWS Microservices Architecture — AWS
- AWS Microservices Architecture - 2
- Azure Baseline — Azure
- Azure Basic Web App Hosting — Azure
- Azure Serverless Web App — Azure

AWS Microservices Architecture ← Prev Next →

✕ Cancel | Submit

4. From the search box, or the scrollable menu of Templates, choose the template you would like to leverage.
5. Click Submit.

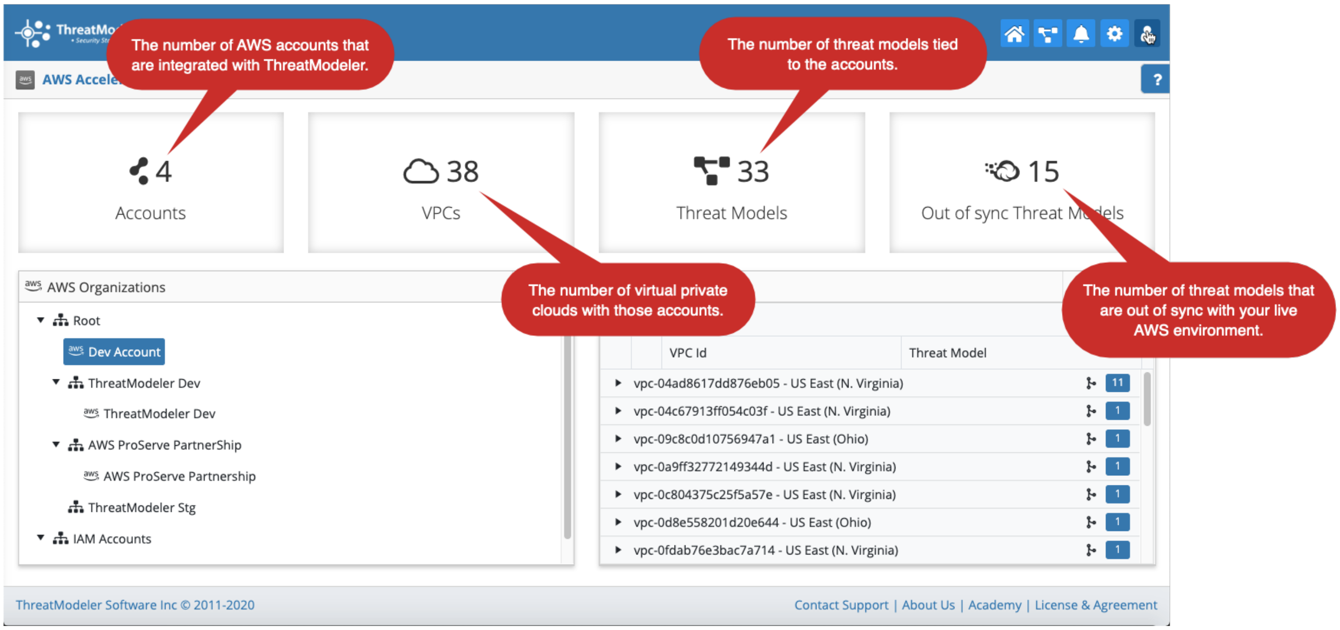
Scenario 5 – User Wants to Review Security Gaps for Deployments in Dev/Test Environments

The user has already deployed applications and workloads in the Dev/Test environments on AWS. In order to identify security gaps prior to pushing these workloads into production, the user should be able to build, manage and maintain a threat model of such Dev/Test environments. Given the complexity of these architectures, building a threat model from scratch can be time consuming.

ThreatModeler's Accelerator for AWS reads the AWS Config to create a threat model for any VPC within the user's AWS Account.

ThreatModeler Accelerator for AWS

1. Click on Settings.
2. Click on aws AWS Accelerator
3. Accelerator for AWS opens with the dashboard – a high-level overview of the organization's threat modeling cloud environment.
4. Once ThreatModeler is integrated with an AWS Account, it uses AWS Config to read all the data for the AWS account and build a threat model. ThreatModeler uses AWS Security Hub to update the compliance status of AWS services that are part of the threat model created using ThreatModeler's Accelerator for AWS.



The number of AWS accounts that are integrated with ThreatModeler.

The number of threat models tied to the accounts.

The number of virtual private clouds with those accounts.

The number of threat models that are out of sync with your live AWS environment.

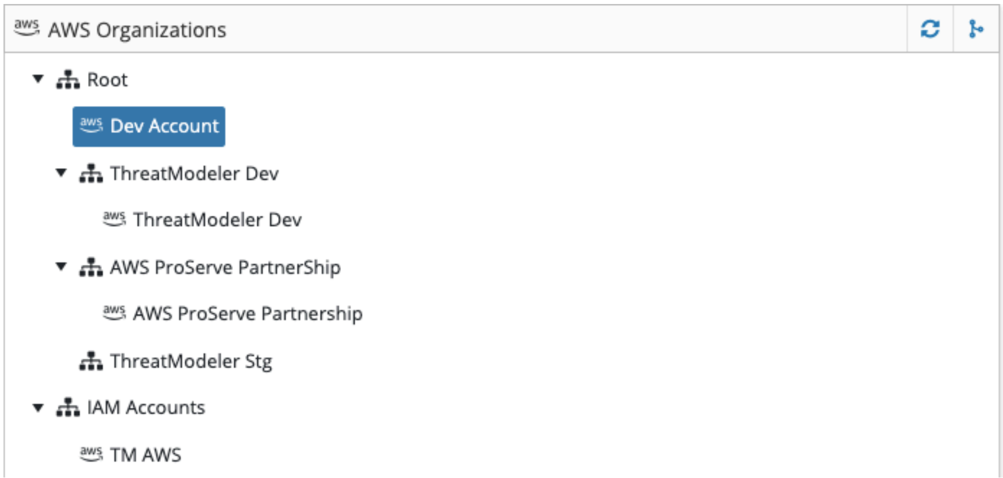
VPC Id	Threat Model
vpc-04ad8617dd876eb05 - US East (N. Virginia)	11
vpc-04c67913ff054c03f - US East (N. Virginia)	1
vpc-09c8c0d10756947a1 - US East (Ohio)	1
vpc-0a9ff32772149344d - US East (N. Virginia)	1
vpc-0c804375c25f5a57e - US East (N. Virginia)	1
vpc-0d8e558201d20e644 - US East (Ohio)	1
vpc-0fdab76e3bac7a714 - US East (N. Virginia)	1

Selecting the Appropriate VPC

Under AWS Organizations, you will be able to see a list of all the accounts that have been integrated with Accelerator and build threat models for VPCs within these accounts.

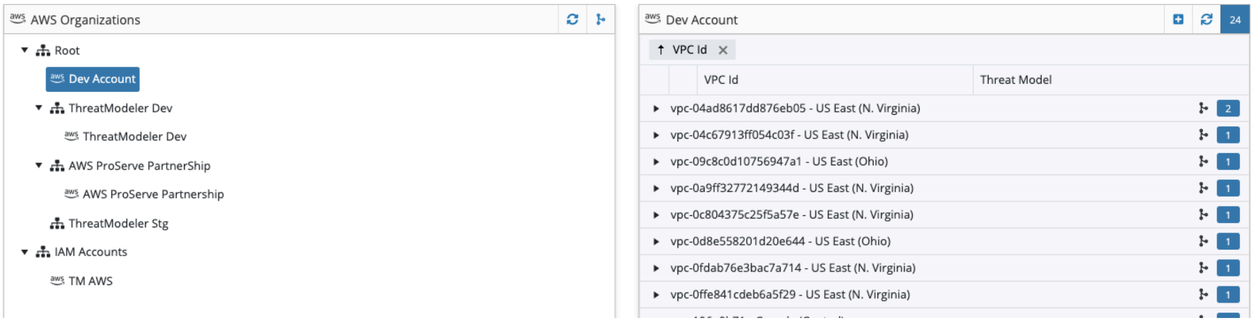
ThreatModeler Account View

1. Click on any account under the AWS Organizations pane. ThreatModeler will list out all the VPCs under that account.



AWS Organizations

- Root
  - Dev Account
  - ThreatModeler Dev
    - ThreatModeler Dev
  - AWS ProServe PartnerShip
    - AWS ProServe Partnership
  - ThreatModeler Stg
- IAM Accounts
  - TM AWS



AWS Organizations

- Root
  - Dev Account
  - ThreatModeler Dev
    - ThreatModeler Dev
  - AWS ProServe PartnerShip
    - AWS ProServe Partnership
  - ThreatModeler Stg
- IAM Accounts
  - TM AWS

Dev Account 24

↑ VPC Id ✕

VPC Id	Threat Model
vpc-04ad8617dd876eb05 - US East (N. Virginia)	2
vpc-04c67913ff054c03f - US East (N. Virginia)	1
vpc-09c8c0d10756947a1 - US East (Ohio)	1
vpc-0a9ff32772149344d - US East (N. Virginia)	1
vpc-0c804375c25f5a57e - US East (N. Virginia)	1
vpc-0d8e558201d20e644 - US East (Ohio)	1
vpc-0fdab76e3bac7a714 - US East (N. Virginia)	1
vpc-0ffe841cdeb6a5f29 - US East (N. Virginia)	1

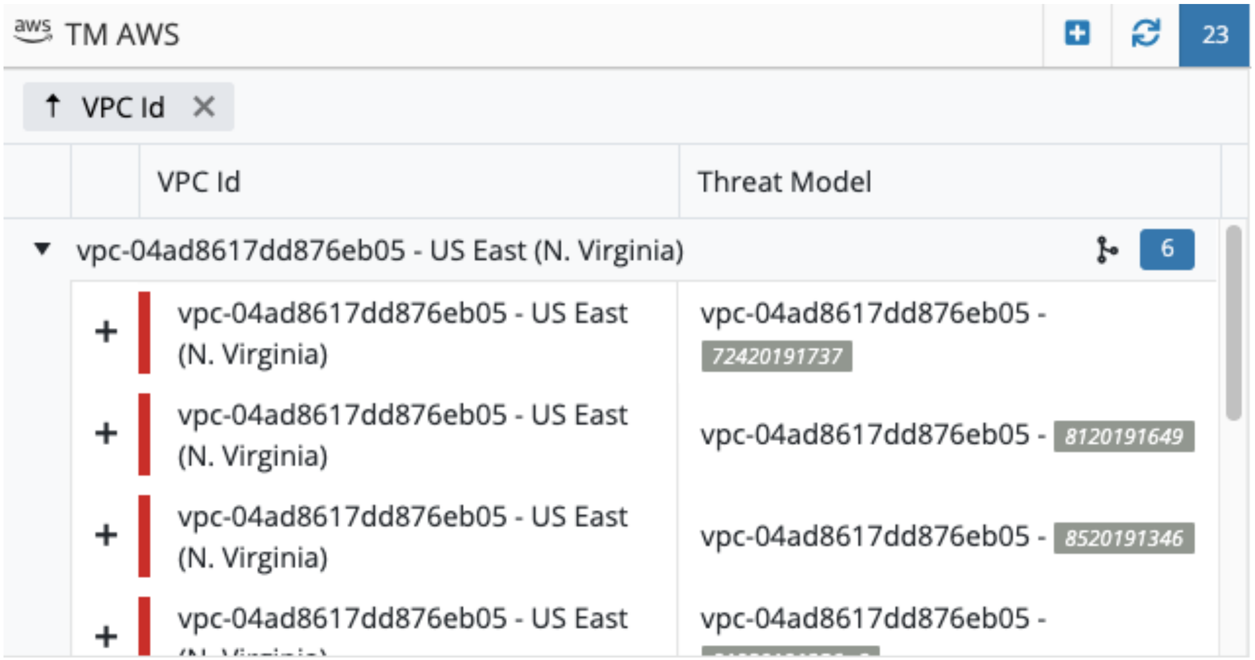
2. You will see a count of the associated VPC threat models and their sync status.
3. AWS Accelerator currently features a one-way sync, which continuously checks the AWS architecture at regular intervals for changes. The sync ensures outputs automatically generated by ThreatModeler are accurate and in near real-time.

AWS Architecture Sync Statuses

- Yellow indicates that a threat model has not yet been created for that VPC.
- Red indicates that a threat model exists, but is currently out of sync with the deployed architecture. This can be due to items included in the threat model

that are not deployed in the live environment, or because the live environment has deployed assets and services that are not identified in the threat model.

- Green indicates that the threat model is in sync with the deployed VPC services.



	VPC Id	Threat Model
▼	vpc-04ad8617dd876eb05 - US East (N. Virginia)	6
+	vpc-04ad8617dd876eb05 - US East (N. Virginia)	vpc-04ad8617dd876eb05 - 72420191737
+	vpc-04ad8617dd876eb05 - US East (N. Virginia)	vpc-04ad8617dd876eb05 - 8120191649
+	vpc-04ad8617dd876eb05 - US East (N. Virginia)	vpc-04ad8617dd876eb05 - 8520191346
+	vpc-04ad8617dd876eb05 - US East	vpc-04ad8617dd876eb05 -

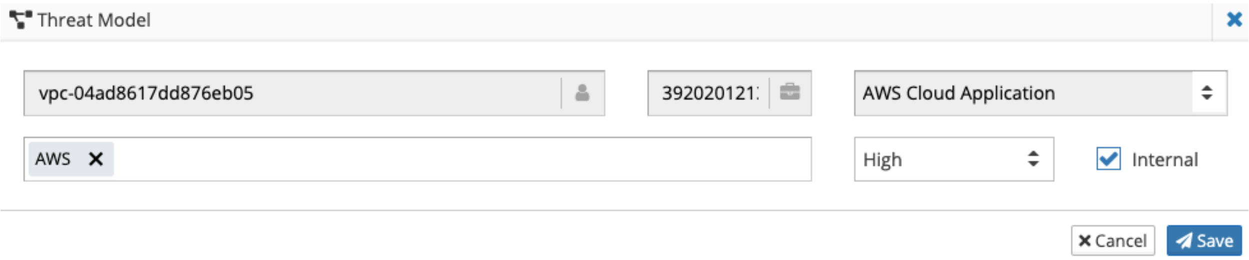
Create a New Accelerator-enabled Threat Model

1. Click on the ▸ icon next to the desired VPC to expand the details of the VPC. Select the VPC which has a Yellow bar.

2. Click on the ⊞ button to create a new Accelerator-enabled threat model. The information will be set to AWS Cloud Application and is unchangeable. Name, Version and Type fields will be pre-set; the Threat Model List Toolbar will also include the:

   - ThreatModeler VPC Number
   - AWS 12-digit ID

3. You can designate whether the Threat Model will be Internal or public facing, set the priority and add labels, which serve as metatags.
4. Click Save.



Threat Model

vpc-04ad8617dd876eb05

392020121:

AWS Cloud Application

AWS ✕

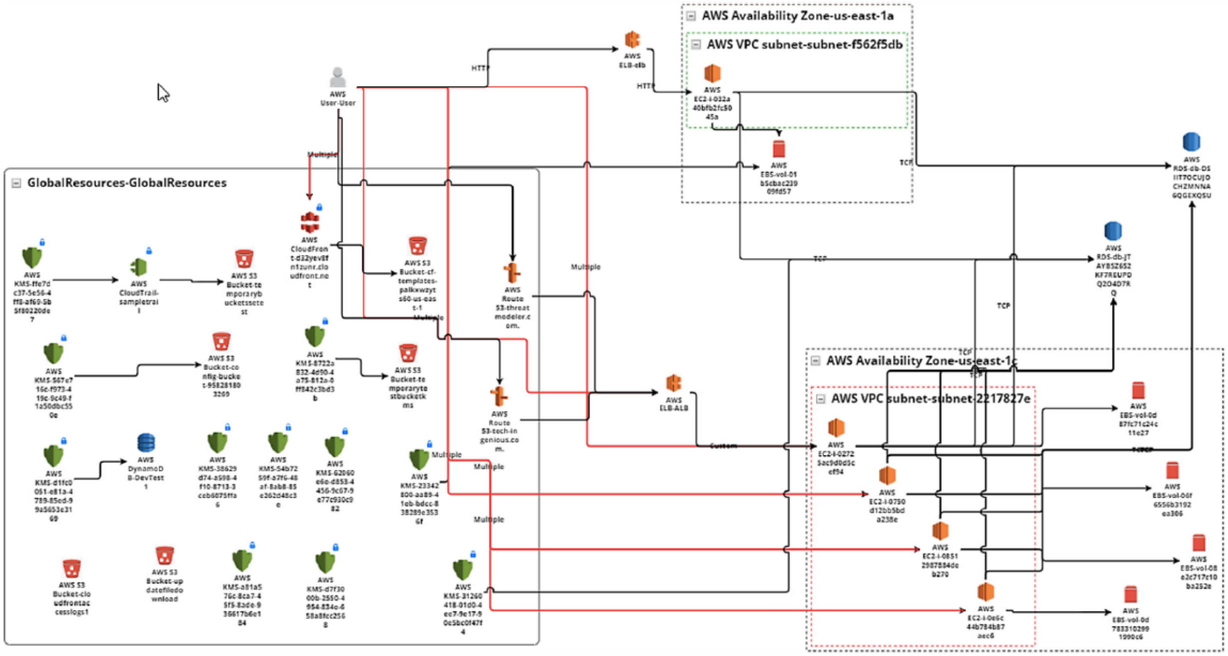
High

☑ Internal

✕ Cancel

Save

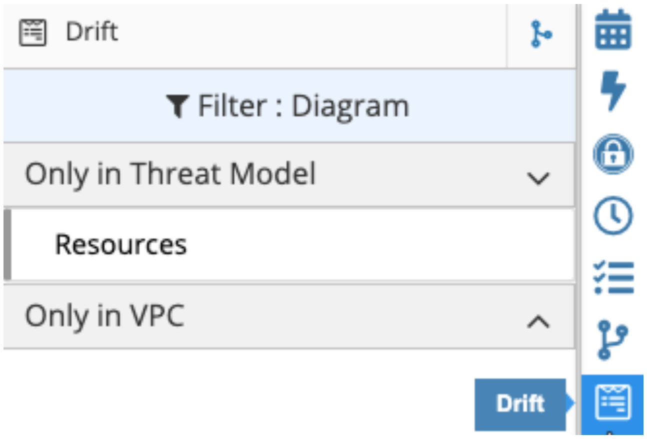
Accelerator for AWS automatically analyzes the live AWS environment, and, within 3-5 minutes, ThreatModeler builds a detailed visual representation of the resources and architecture currently deployed.


AWS Availability Zone-us-east-1a
AWS VPC subnet-subnet-f562f5db
GlobalResources-GlobalResources
AWS Availability Zone-us-east-1c
AWS VPC subnet-subnet-2217827e
HTTP
TCP
Multiple
Custom

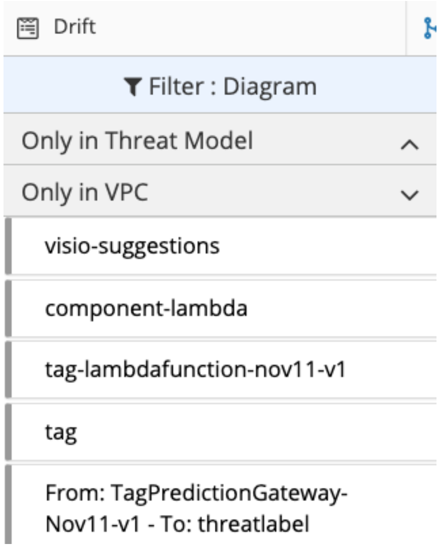
Analyzing Deployment Delta Using Drift

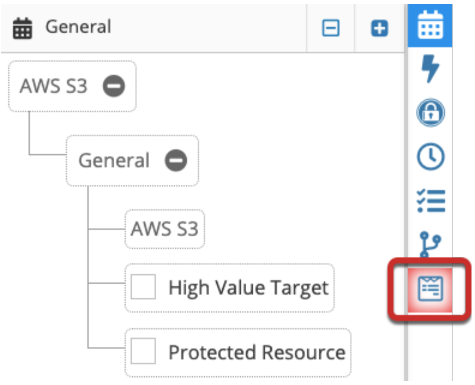
Once a diagram is created using Accelerator, you can continuously monitor any alterations to your cloud environment by analyzing the Drift.

1. Click on the Drift Log icon to pull up the sync report.

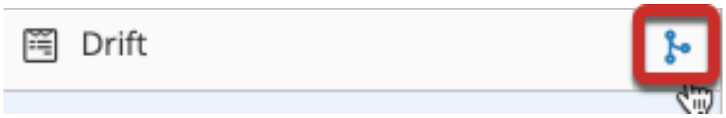


2. If there are additional updates or changes made in AWS, Drift enables you to sync the information and update the ThreatModeler diagram with any changes identified in your architecture.
3. As indicated in the screen shot below, you can filter the diagram based on what is "Only in Threat Model" vs. "Only in VPC." With the filter, you can see what components are missing in order to sync them.





4. After completing your analysis, click on the Sync button. ThreatModeler will automatically analyze the live AWS environment and bring the current threat model back into sync with the deployed environment based on the latest VPC architectural deployment.



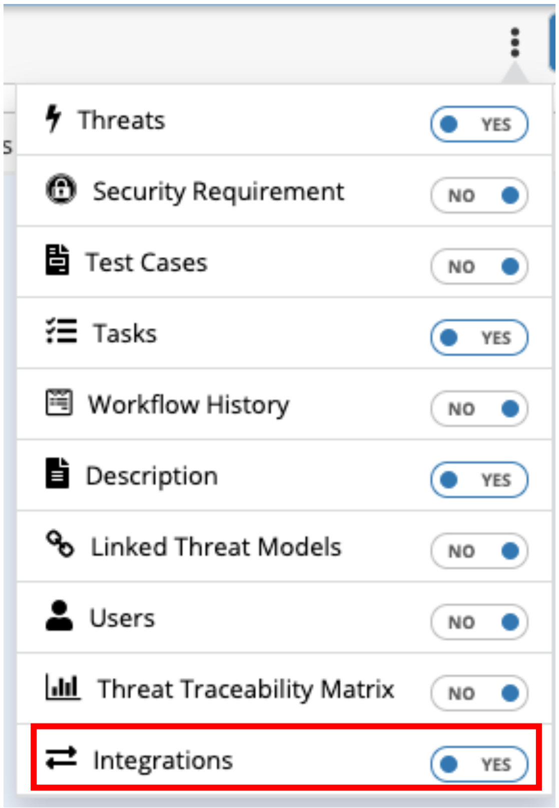
Scenario 6 – User Wants to Measure and Manage Progress of Security Epics Implementation

Continuing on from the activity of building threat models, a user should be able to measure progress when it comes to implementing Security Epics within the AWS environment. As a process, each threat model should be able to provide the user with insight into actionable security requirements. These security requirements should further become part of a project's backlog and, once implemented, a validation helps to provide an understanding of compliance with standards such as CIS.

Integrating with Issue Tracking tools (e.g., JIRA)

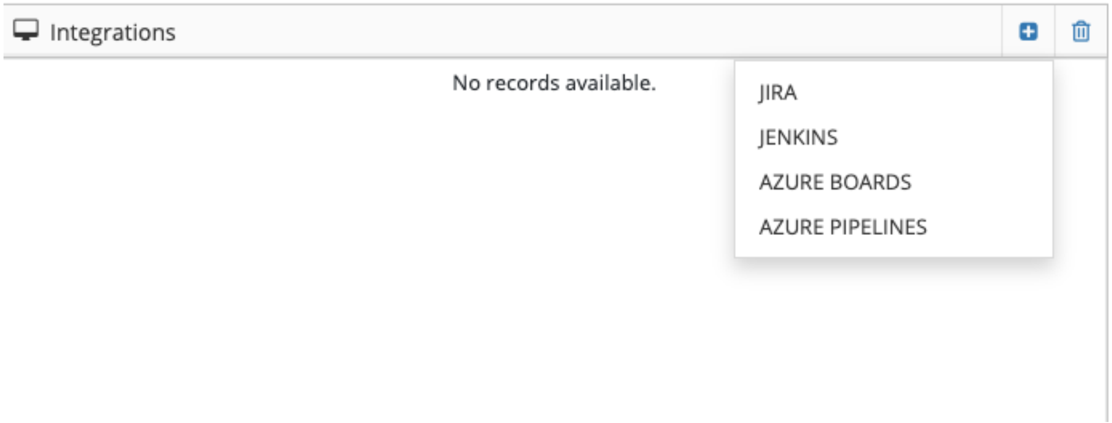
Once a threat model is built in ThreatModeler, a user can push security requirements into issue tracking tools such as Jira. To do so, follow these steps:

1. Navigate to the Overview screen of your threat model.
2. On the top right, click on the ⋮ button.
3. Toggle the Integrations switch to Yes by clicking on it.



Threats: YES
Security Requirement: NO
Test Cases: NO
Tasks: YES
Workflow History: NO
Description: YES
Linked Threat Models: NO
Users: NO
Threat Traceability Matrix: NO
Integrations: YES

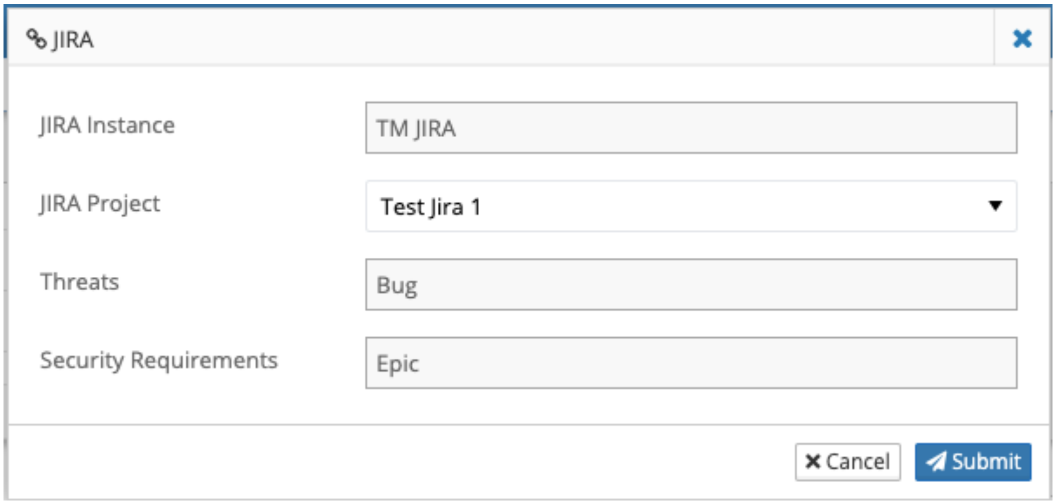
4. Scroll down to the Integrations pane, click on the ⊞ button and select Jira.



Integrations

No records available.

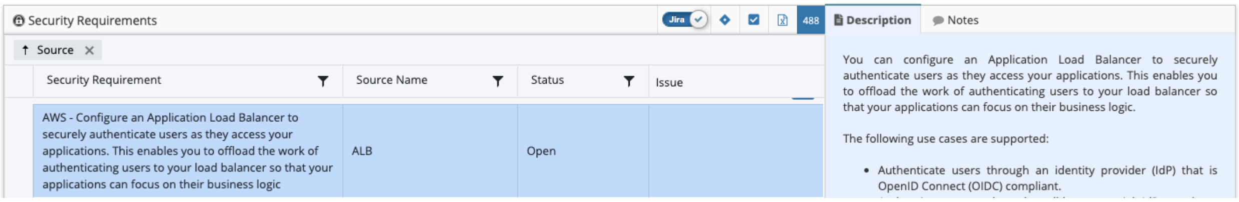
5. This will open a pop-up window asking for project details within Jira. Select the Jira instance, Jira project, and how threats and security requirements will be reported within Jira. Hit Submit.



JIRA

JIRA Instance	TM JIRA
JIRA Project	Test Jira 1
Threats	Bug
Security Requirements	Epic

6. Once the threat model is linked to Jira, you will see a Jira toggle on the Threats and Security Requirements pane. Now select any security requirement and create an issue by clicking on the ◆ button.
7. Hit Save after reviewing ticket details to assign the Jira ticket ID against the security requirement.



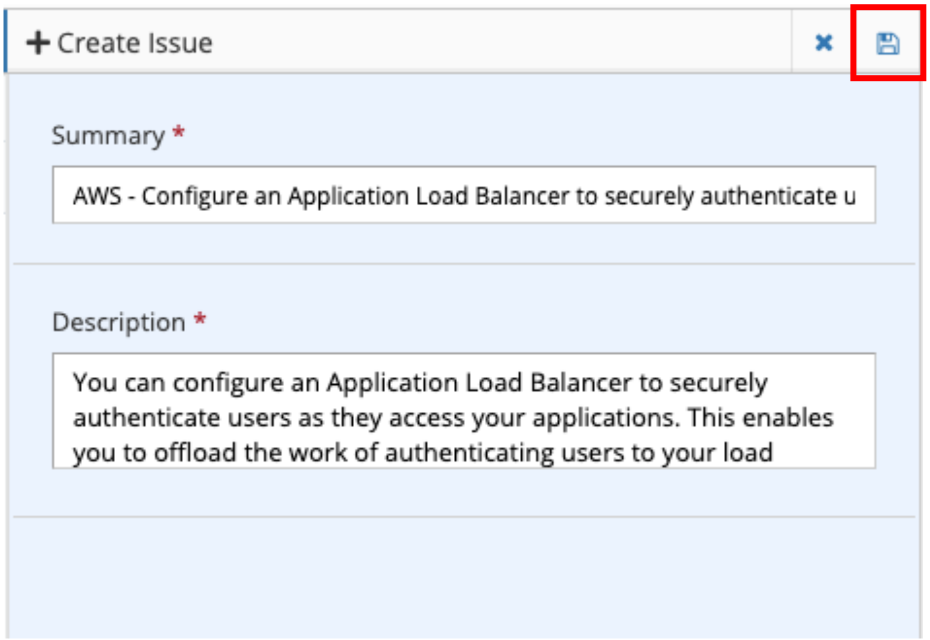
Security Requirements

Security Requirement	Source Name	Status	Issue
AWS - Configure an Application Load Balancer to securely authenticate users as they access your applications. This enables you to offload the work of authenticating users to your load balancer so that your applications can focus on their business logic	ALB	Open	

You can configure an Application Load Balancer to securely authenticate users as they access your applications. This enables you to offload the work of authenticating users to your load balancer so that your applications can focus on their business logic.

The following use cases are supported:

- Authenticate users through an identity provider (IdP) that is OpenID Connect (OIDC) compliant.



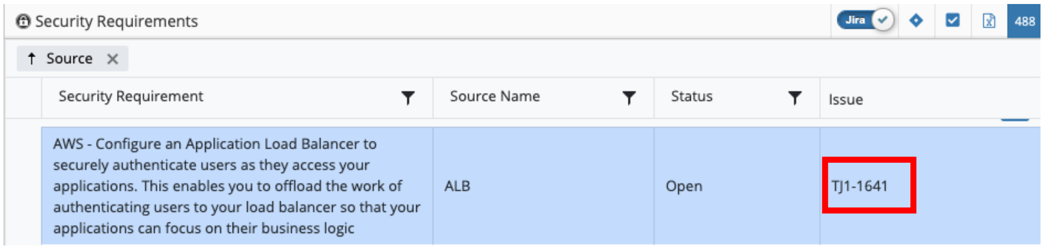
+ Create Issue

Summary *

AWS - Configure an Application Load Balancer to securely authenticate u

Description *

You can configure an Application Load Balancer to securely authenticate users as they access your applications. This enables you to offload the work of authenticating users to your load

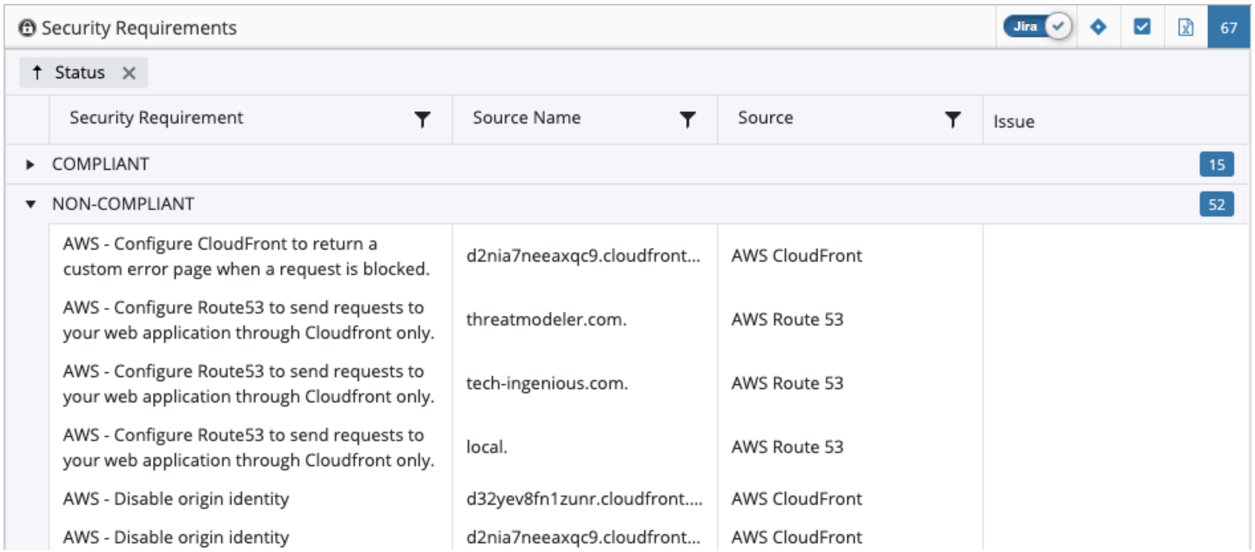


Security Requirement	Source Name	Status	Issue
AWS - Configure an Application Load Balancer to securely authenticate users as they access your applications. This enables you to offload the work of authenticating users to your load balancer so that your applications can focus on their business logic	ALB	Open	TJ1-1641

8. Once a status is changed within Jira for the respective ticket ID, it will track back into ThreatModeler as a status change for the security requirement.

Validating Security Epics

When looking at Accelerator-built diagrams, ThreatModeler validates the implementation of Security Epics through its integration with AWS Config and AWS Security Hub. You will notice that security requirements have statuses such as “COMPLIANT” or “NON-COMPLIANT,” which give users visibility into the implementation.



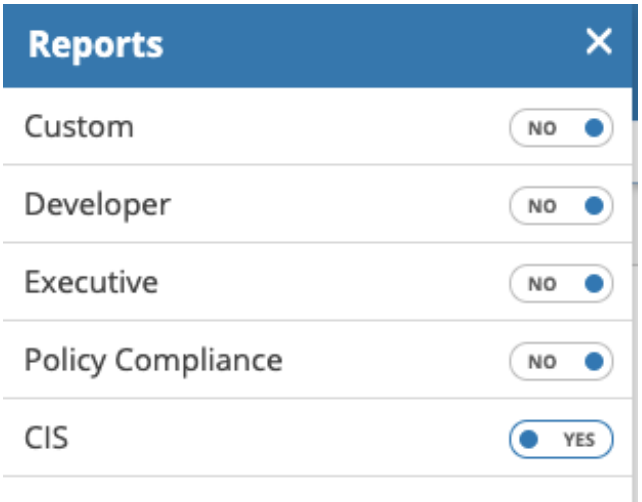
Security Requirements

↑ Status ×

Security Requirement	Source Name	Source	Issue
▸ COMPLIANT			15
▾ NON-COMPLIANT			52
AWS - Configure CloudFront to return a custom error page when a request is blocked.	d2nia7neeaxqc9.cloudfront....	AWS CloudFront	
AWS - Configure Route53 to send requests to your web application through Cloudfront only.	threatmodeler.com.	AWS Route 53	
AWS - Configure Route53 to send requests to your web application through Cloudfront only.	tech-ingenious.com.	AWS Route 53	
AWS - Configure Route53 to send requests to your web application through Cloudfront only.	local.	AWS Route 53	
AWS - Disable origin identity	d32yev8fn1zunr.cloudfront....	AWS CloudFront	
AWS - Disable origin identity	d2nia7neeaxqc9.cloudfront....	AWS CloudFront	

Generating Compliance Reports

On the Reports tab for a threat model project, a user can check compliance with the CIS benchmarks for threat models built via Accelerator.

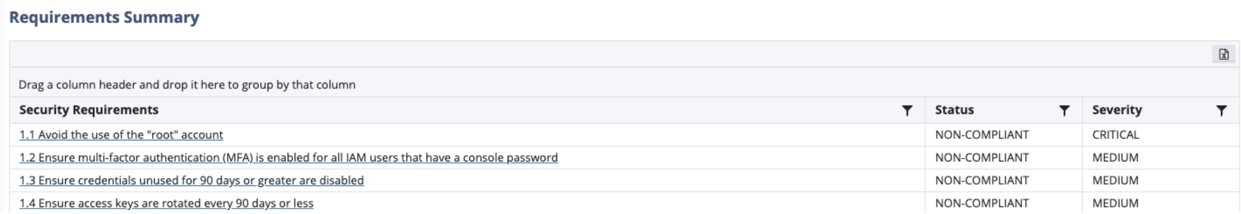


Reports ×

Custom	NO
Developer	NO
Executive	NO
Policy Compliance	NO
CIS	YES

The CIS report shows two statuses: COMPLIANT and NON-COMPLIANT. ThreatModeler automatically displays the compliance posture of a threat model based on the CIS compliance information from AWS Security Hub. As you build out the threat model using Accelerator for AWS, ThreatModeler will update the status. Different statuses include:

- Compliant
- Non-Compliant



Requirements Summary

Drag a column header and drop it here to group by that column

Security Requirements	Status	Severity
1.1 Avoid the use of the "root" account	NON-COMPLIANT	CRITICAL
1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	NON-COMPLIANT	MEDIUM
1.3 Ensure credentials unused for 90 days or greater are disabled	NON-COMPLIANT	MEDIUM
1.4 Ensure access keys are rotated every 90 days or less	NON-COMPLIANT	MEDIUM

Summary

In summary, a user who wishes to establish a threat modeling process at an organization should be able to build a cohesive architecture, which provides insight into relevant controls under the Security Epics. These controls should be actionable in that they become part of the project’s backlog and further verifiable from the source.

Moreover, the process of threat modeling should be a repeatable exercise to ensure standardization within the organization. Therefore, any user should be able to build and maintain a repository of pre-approved design patterns.

For more details around additional use cases, please feel free to access the Interface Guide.