IriusRisk

Solution Brief

Using Infrastructure as Code (IaC) to Accelerate Threat Modeling

Key Challenges

Companies fail to include secure design analysis in their System Development Life Cycle (SDLC) because it requires security experts that are in short supply and because it includes manual, time consuming steps, like drawing the diagram and including all the required meta-data. This manual approach takes too much time and is incompatible with modern agile development practices. As a side effect, threat modeling is limited to applications with a high requirement for assurance and security.

Infrastructure as Code (IaC) has significant benefits in alleviating challenges with cloud-based services - allowing the manual provisioning of infrastructure to be automated, repeatable and consistent and allows DevOps to focus on doing what they are best at: the software development lifecycle. However, it also represents several challenges - IaC doesn't necessarily guarantee secure environments - issues such as configuration 'shift' can occur when services need urgent implementation yet the necessary infrastructure defined by IaC may not be available.

Some core challenges include:

Lack of integration with existing DevSecOps processes, meaning entire departments wasting valuable time and skills

Real-time collaboration between teams is practically non-existent

Monitoring threats and weaknesses is difficult and often lies within several departments and across multiple systems - no central place to view, prioritize and action

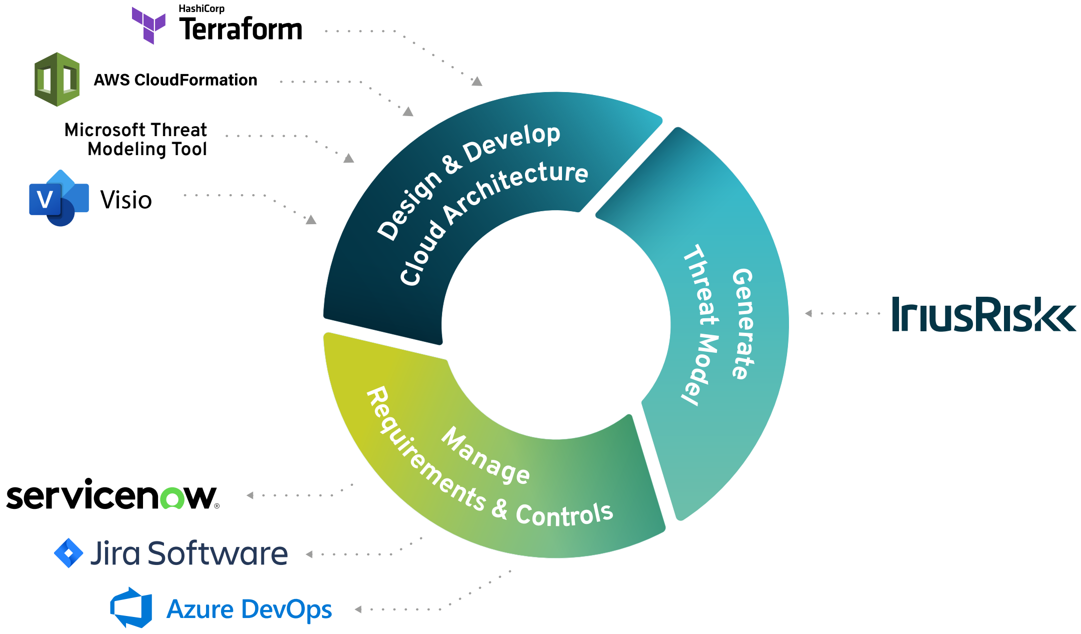
Solution Overview

Automated Threat Modeling of IaC environments during the architectural and design phases allows DevOps teams to understand and manage their environments more securely by constant monitoring of evolving threats and vulnerabilities through to consistent checking of IaC definitions across the whole of the AppSec and DevOps environments.

IriusRisk's most recent release of the Automated Threat Modeling platform has been designed to make it easier than ever for teams to generate threat models of cloud native designs. Customers are able to generate a threat model from IaC descriptors, such as AWS CloudFormation, HashiCorp Terraform, Microsoft Visio and Microsoft Threat Modeling Tool with the model containing the applicable threats and prescriptive security controls.

How it works

Our platform allows cloud native designs to be automatically analyzed from a security perspective without having to manually draw the architecture diagram. IriusRisk generates a threat model from an Infrastructure as Code (IaC) descriptor, and this model will contain the applicable threats and prescriptive security controls. The IaC code provides an excellent opportunity to answer the first question of Shostack's approach for threat modeling in an automatic way: "what are you building?". After the IaC code is imported into ACSDA, we can take advantage of the rules engine to automatically see the main threats related to that architecture.



Key Benefits

Cloud architectures can be simply and effectively threat-modeled (through IaC and APIs)

Allows **real-time Threat Modeling Collaboration** across different geographically located teams

Application security can be **owned and integrated** by the **whole SDLC process** from architecture, through to Developers, through to security

Why IriusRisk

IriusRisk was designed to scale threat modeling to the thousands of applications that large enterprises create and maintain every year using automation and threat libraries. IriusRisk's software automates and manages the threat modeling process collaboratively, bringing security architects and developer teams together.

To generate a threat model, users of IriusRisk need to input the architecture of the system using a diagramming tool and some additional meta-data.