CASE STUDY

# Multinational financial services firm sustains threat modeling practices with threat modeling automation platform

## Company background

The company is an American multinational financial institution with a decentralized threat modeling practice where each division has their own process for threat modeling applications and non-shared infrastructure. With an ever-evolving threat landscape, the customer finds that creating a global threat modeling process is difficult to get consensus on- and even more difficult to sustain and scale. They have identified a need to centralize their teams into a single platform with visibility for key stakeholders and automation to reduce the time to threat model while providing critical scalability for the many applications that need to be threat modeled in the coming months.

## Challenges

- No standardized approach to building threat models leading to different outputs
- Lack of centralized reporting making it difficult for senior leadership to visualize risk levels for budgeting and forecasting
- Current process is not scalable (even within each division) and expected work is unlikely to be completed according to schedule.
- Application security expertise varies from division to division producing quality differences between threat models

## Solution

Company decided to implement IriusRisk's Threat Modeling Solutions and Analytics Module for advanced dashboarding and reporting.

## Key features and benefits of IriusRisk

- Centralized Platform to provide for a single hub where all divisions can produce and store threat models while providing the protection and segmentation into the threats and expected countermeasures between division threat models
- Integrated Business Intelligence: With the analytics module integrated into the core product, key stakeholders are able to query all of the SaaS data directly and build role specific dashboards and reports that report on real time information
- Tool sustained processes: Enabling a tool to make the right process the only process enables organizations to sustain and grow critical threat modeling processes without needing to police those processes

IriusRisk

- Library integrated: Leveraging a centralized threat library ensures that each threat model has a consistent level of expertise and threat scenarios under consideration
- Automated IaC imports: Fulfill expected workloads through the import of Infrastructure as Code files into IriusRisk. Using the Terraform and Cloud Formation integrations to build threat models directly from code enables teams to accelerate threat modeling using like for like representations of their infrastructure.

## Implementation plan

- Onboarding: Company works with IriusRisk's Customer Success team to review current processes and design a tailored onboarding plan that reflects customer objectives and key features for implementation. These processes are documented with the customer and rebuilt within the new tool.
- Training & Support: Customer success team provides virtual or direct training for administrators, content creators, automation teams, business intelligence team members, and front line managers on solutions.
- Integrations: Customer success team and product support team works with customer teams to enable customer prioritized integrations with third-party services such as Terraform, CloudFormation, and others.
- Preliminary Rollout: Several divisions are selected for internal rollout to test new processes.
- Scaling & Automation: Upon successful implementation of the solution in the trial divisions, product is rolled out to remaining divisions.
- Continuous Improvement: IriusRisk periodically meets with the customer to review progress and process to determine how the product can be continually adapted and improved.

## Expected outcomes

- New and existing processes are sustained and enabled by the threat modeling product.
- Threat Modeling process have been built to scale inside of a new platform
- Consistent expertise: leveraging the IriusRisk risk pattern libraries ensures that each threat model has consistent cybersecurity and best practice outputs.
- Greater visibility: Leadership and stakeholders have access to the right information when they need it without requiring extensive training or reporting assistance.
- Integrated & centralized solution that provides downstream extensibility into teams and upstream integration into infrastructure reducing non-value added processes.