CASE STUDY

Multinational conglomerate partners with IriusRisk to measure and identify unknown attack vectors and potential vulnerabilities across applications.

THE REQUIREMENT

Identify unknown attack vectors and potential vulnerabilities within products

Multinational conglomerate required further documentation and effective technology to measure their security efforts, especially as the products are between five and 15 years old. The team were looking for ways to identify unknown attack vectors and potential vulnerabilities that may otherwise be missed within these legacy-type of products. They had 7 complex products to threat model.

THE SOLUTION

Find the tool—connectivity of components and vulnerabilities

This led the team to look for a threat modeling tool, to be able to create architecture diagrams, identify the threats, and see all the connectivities between assets and components. This single view is effective for the whole team to have visibility of the company's products. IriusRisk threat modeling has made the development team more aware of the things they should be worrying about by providing insights and priorities - connectivity of components and vulnerabilities - and how the product is being utilized by clients. For the multinational conglomerate to be able to forecast risk and fix it in advance saves a lot of time.

Positive outcomes and the IriusRisk tool

There have been multiple positive outcomes since using IriusRisk, some of which include:

- Identification of potential opportunities for evolution, improvements, and fixes
- Improved visibility of how the resources are deployed, enabling actions to optimize costs and resources
- Enhanced collaboration between teams
- Identification of potential architecture-related risks, allowing adoption of appropriate mitigation strategies
- Enhanced security by identifying vulnerability points and implementing protective measures

The challenges with rollout

The team responsible for rolling out this new technology had no prior threat modeling experience. On top of this, they had incredibly complex diagrams to build for their threat models, with nested components, dataflows, tagging requirements, plus a large number of actual components. In addition, having one core user as the owner and trainer was a large responsibility.

Collaborative Effort

The threat modeling initiative was a collaborative effort across various units, including Legal, Tax, and others. Software Architect focused on the solutions within the Legal One unit, whereas Information Security Manager was the coordinator who led the initiative across the teams. The mixture of areas and roles aided in team understanding and likelihood of adoption.

Documentation

Security Champion built out his own documentation based upon what IriusRisk provides, and created a full report to demonstrate use cases for IriusRisk. The Champion even listed the pros and cons of the technology to aid other teams that may adopt the software to further provide Multinational conglomerate specific documentation.

Improved Compliance

Ability to define metrics that the organization needed, and promote a security risk approach demonstrating compliance considerations at the same time.

Augmenting existing security processes

Better processes for production, development and security teams. Qualys, Snyk, Veracode and penetration testing were previously used for identifying vulnerabilities, now with threat modeling these other investments are further streamlined and all work collaboratively.

High level of threats

IriusRisk's role is to clearly highlight all the possible threats, teams would then need to prioritize them according to the environment and objectives. With a new and improved UI from IriusRisk, Admins will now have more tools to help in triaging and filtering the threats appropriately.

Team engagement

Some challenges to bring teams on board on another technology, however once results are demonstrated this engages individuals and they are keen to learn.

Conclusion

The multinational conglomerate has made excellent strides with IriusRisk, thanks to the efforts and dedication of its collaborative effort across teams. The multinational conglomerate has now 7 threat models of complicated applications, with the experience and process in place to roll out across other geographies. From a security perspective, Multinational conglomerate now has a more accurate view of its applications and associated threat landscape.