IDT Innovative Digital Transformation

Meta Data Protection Assessment

IDT helps Game development company successfully pass Meta's DPA and revisit their security practices

Executive Summary

A European-based game development company was looking to maintain their new flagship product on the Meta platform after receiving notice of the need to complete the Meta Data Protection Assessment (MDPA). They contacted IDT in an effort to accelerate their response to the MDPA, which is a requirement to access user data on the Meta platform. IDT produced a contract and reached an agreement in less than two weeks, and within days was on boarded and delivering. 45 days later, the IDT team had submitted the MDPA questionnaire with required artifacts on behalf of the customer and received approval, derisking the customer's relationship with Meta. IDT's comprehensive approach to the MDPA response ensures that the customer is supported throughout the assessment process until approval is received.

Introduction

Mobile game development is a rapidly growing market offering opportunities to the organizations that can get to market with speed and quality. With those opportunities come new challenges such as the constant need for acquisition of new users, which is fulfilled through integration with major social platforms. The platform providers, like Meta, have put strict compliance requirements and regulations in place to govern the applications using the platform data APIs.

IDT was approached by a European software company that specializes in the development and support of mobile online games. They were seeking a reliable partner who would help them prepare for the Data Protection Assessment conducted by Meta prior to the go-live of their mobile gaming application go-live.

The Challenge

Data Protection Assessment is a Meta requirement for apps accessing data provided by the Facebook platform integration (Platform Data). That data consists of personal information of the Facebook users and can be used for various needs such as user authorization and collection of statistics. The assessment is designed to determine how exactly the developers use, share, and protect Platform Data. During the assessment, the owner of an application (mobile game, in the given case), must fill out a questionnaire based on their app's access to the Facebook data, and provide evidence for their answers demonstrating that the company maintains certain practices to keep the data secure. The 60-day timeframe for the assessment can be challenging for organizations to meet on their own, and failure to meet the deadline risks the loss of platform access and the revenue associated with it.

IDT Solution

The customer's cloud-based application is hosted on infrastructure in AWS and Google Cloud, so the engagement started with a technical security assessment of both environments to determine how close they conform to cloud security best practices and build a custom remediation plan tailored to the customer to improve their security posture.

In parallel, IDT's consultants engaged the customer's technical, management and legal teams in multiple conversations, discussing various aspects of the application and the company as a whole including:

- Architecture of the application and its underlying cloud infrastructure.
- The Privacy classification of end user data provided by the Facebook platform, its flow through the organizations system, storage, and encryption.
- Internal company practices and established processes regarding the treatment of sensitive data, logging & monitoring, incident detection & response, staff responsibilities, compliance with standards & regulations, etc.

Next, the IDT team implemented an iterative approach to discovery and remediation, allowing the larger remediation steps to be executed while the IDT team completed the questionnaire and artifacts required for the Meta DPA. As an additional deliverable, the IDT team built a comprehensive long term security strategy with runbooks and operational guides for the customer teams.

Once the questionnaire was submitted to Meta, our team switched focus to enabling the customer technical and legal teams to adapt to the new tools, processes and technologies that were put in place as part of our engagement.
Our customer submitted the completed Meta Questionnaire. While awaiting response from Meta's assessors, IDT conducted work sessions with our customer's Technical and Legal teams to ensure that they were ready to start adopting and using the new policies and practices.
As with most assessments, Meta assessors requested additional evidence not mentioned in the main MDPA. IDT conducted additional working sessions with our customer to determine the details and prepare the appropriate documentation. After submission of the additional evidence, Meta was satisfied and responded with final approval within the 60 day timeline.

Benefits to Client

As the main output of the engagement, our customer passed the Meta Data Protection Assessment and got their application approved for integration with the Facebook API. With the information collected through the discovery process, IDT was also able to produce a full report containing the customer's security posture with a straightforward backlog that can be used to further advance the customers security and compliance posture.

Lastly, our customer received a ready-to-use set of security-related policies, procedures, and runbooks to assist with incident response, increase security team capabilities, and ensure business continuity.