Mindtree helps one of the world's leading electronics manufacturer secure its remote appliance connectivity solution

Abstract

In the age of Internet of things (IoT), remote connectivity with appliances is key to handle and monitor applications and appliances from any location of preference. Furthermore, all connections established between the host and clients must be tightened through encrypted and proactively-managed security. So, when a global electronics manufacturer wanted to secure its latest remote connectivity solution while ensuring regulatory compliance and reducing IT costs, they turned to Mindtree for an expert solution.

Challenge

The manufacturer understood the risk of having its remote access applications being exploited by a third party. Any breach in the information flow could lead to denial of service, system downtime or even compromise customers' sensitive data. Such incidents were reported from other service providers, leading to huge ransom payments leaving a negative impression on the business. The manufacturer needed prime identity management and end-point security solutions to secure information flow system for remote application connection enablement systems.

Solution

Mindtree delivered end-to-end security solutions encompassing the Identity Management and Security

services and the Application Security services to tackle the challenge faced by the client (as shown in the process flow). The activities carried out in this exercise included:

- Understanding the tech stack and creating attack vectors based on known threat models
- Classifying the vulnerabilities at the architecture level and drawing up attack simulations
- Integrating the most influential security frameworks and the Mindtree security arsenal
- Attacking security implementations by creating exploits and POCs for each vulnerability
- Achieving the optimized security for IoT solution on cloud infrastructure including web and mobile applications
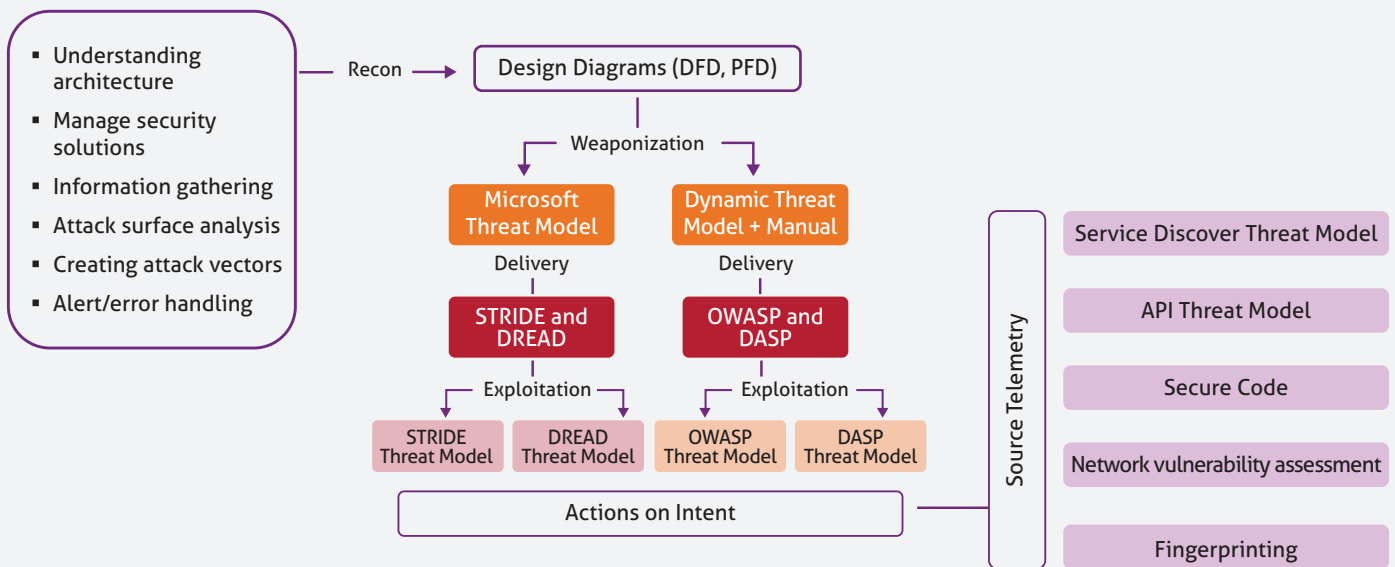
These steps unveiled over 50 critical system vulnerabilities and could have amounted to the leakage of sensitive personal data of users using the connectivity solution of the client.

To monitor future attacks, a vulnerability management portal was created to help reduce duplication of vulnerabilities and provide real-time network health.:

Impact

- The security solution provided by Mindtree secured the sensitive personal information of over 100,000 users on-boarded on the platform that could have otherwise been exposed to a third party without user consent.
- This serious threat for the customer information stored in the company database could have damaged the company's reputation.
- Implementing Mindtree services, the company saved millions of dollars in ransomware damages.