apisec.ai

Health Tech Firm Case Study

Health Tech Firm adopts apisec™ achieving Default Secure API with 1 month ROI

Introduction

Our client, A Health Tech Firm is a revolutionary on-demand health insurance company that has the vision to make health insurance more effective and affordable. Formed in 2017, The client took on the major challenge of health insurance, which is a highly protected area under HIPAA and privacy laws. The client has built its offerings around APIs that allowed web, mobile and direct access to the information related to health care options. The client provides its services to many companies in the Fortune 500, having very high expectations on The client's data security.

Challenge

Having started the disruptive healthcare company in a tight privacy driven market the client team knew they had to start with a default secure mindset. They began by looking at all the fundamentals of DevSecOps namely dynamic analysis, static analysis, RASP. They went to evaluate a containerized stack with a focus on Mobile First.

The CISO of our client was early in the journey and he knew the engineering team and processes would mature quickly so he had to get the easiest to consume solution in place for engineering teams to adopt. The engagement with apisec™ started very early on. The CISO could see the challenges of business logic vulnerabilities and the conflict between releasing software quickly and the need to fully validate. He knew that the right answer was an automated integrated solution into the development toolchain.

Developers are great at getting working products out of the door quickly, getting every developer accustomed to security, learning how the hackers will try to compromise the APIs, is not something that every developer would know, nor they must be forced to learn. Security has to be built into the development process. Moreover, when the breaches are at the business logic layer, traditional static code analyzers can't mitigate the risk.

"After working with apisec.ai, our technologists were impressed with the approach and capabilities. Today it is our biggest bang for our security buck." The Health Tech Firm CISO

Solution

apisec™ Automated API risk discovery with integrated DevSecOps.

The clients security team brought apisec™, but they knew they needed to get the developers on board, they needed to make the solution easy to consume, without causing friction with the existing development processes or tools.

Key Benefits

- CI/CD pipeline integration of API Security for quick discovery of flaws
- Business Logic Layer API Security testing and certification allows team to focus on building great products
- Shift Left of Security team enabling better understanding the needs to security by development team

Health Tech Firm Case Study

apisec™ began with an automated API risk discovery, with the Swagger definition file. Consuming this definition, the solution built the API feature map automatically, all the way to the business logic layer. Then the BOTs are unleashed to build custom security attack vector creation to uncover all the business logic including RBAC, ABAC, Application DoS attacks and injection flaws that hackers could use.

apisec™ was first introduced into the staging environment scanning, prior to the clients application would go live to find critical vulnerabilities. Once the categories were enabled the AI-based matching and categorization process began. The attack vectors were injected in, the AI-driven exploit reporting and remediation engine began to highlight the most critical issues and suggestions on how to solve.

As the security team saw the issues, they wanted to bring engineering directly into the process, without having to duplicate the issues, creating tickets in the engineering systems and then going back and forth on issues was cumbersome. Hence, the decision was made to integrate directly into the clients defect management system.

After demonstrating the value of the system and early detection to the QA lead, the decision was made to integrate directly with the CI/CD pipeline. Allowing for a shift left execution of the apisec™ solution and also a shift right by including production into the DevSecOps journey to be brought deeply into the security validation of the solution.

Our client recognized that even with the BOTs creating the playbooks there was knowledge about the endpoints that only the client engineers would have. They were able to use the Security category authoring with code-less threat modeling to extend the coverage of their endpoints. This was a huge advantage which then allowed our client to share these with the Community of apisec™ customers for their own use.

apisec™ had the ability to provide very rich information on each API vulnerability that was uncovered, resulting in less time by developers to understand the issues, allowing for their precious time to be focused more on fixing issues and enhancements.

The team at our client is able to rely on apisec™ for all of their API validation requirements, due to the product's ability to execute validated request and response with an AI-driven Matching and Categorization engine. As the development team changes the API as needed, the apisec™ solution automatically discovers the added API features, rebuilds the API feature map and then re-launches the BOTs to create new attack vectors. Our Client has achieved a highly secure API-First development with 1/10 the cost of less effective approaches. Currently, Our Health tech client uses apisec™ for more than 1M assessments per month per API to ensure that the highest security standards are followed into each commit.

Conclusions

apisec™ is able to bring API security to our Health Tech client at a fraction of the cost of manual methods, bringing in coverage and protections at the speed of their development.

To learn more about how apisec™ can add security to your API by default and allow your precious resources to be focused on developing faster.

Please visit apisec @

https://www.apisec.ai/defaultsecureAPI