CYBER HARDENING FOR LEGACY SYSTEMS

Program Overview

Cyber security is a concern for every software system. More than ever before it is critical to analyze software security earlier and throughout the development process. Tangram Flex developed configurable API hardening tools to improve cyber security of our customer's continuous development (CI) / continuous delivery (CD) pipeline.

These cyber assurance tools allowed our customer's engineering team to detect and respond to vulnerabilities earlier in their software supply chain.

Technical Approach

Tangram Flex's engineering team selected and implemented three types of API hardening to best serve our customer's mission-critical need:

Endpoint Hardening
protecting applications from unexpected or undefined information

Payload Hardening
defining the data an application should expect so it knows what to reject

Port Hardening
preventing the unintentional exposure of API information

Tangram's API Hardening solution is extensible to other aspects of our customer's CI/CD environment. It can be used to secure their entire software development pipeline. Currently our customer's engineering team is using custom Tangram-built tools to secure messaging between applications.

Tangram Engineering Expertise

Tangram Flex provides game-changing capabilities for digital engineering. Our core product, Tangram Pro™, automates manual and labor-intensive software integration processes. We are the leading provider of software assurance, reducing the time and skill-level needed to produce assurance data, documentation, and certification. Tangram Pro™ helps bring capabilities from concept to warfighter at a relevant and responsive pace.