

DevSecOps and Traffic Analysis

Introduction

The DevSecOps process focuses on security in the software development lifecycle and integrates code development with operations and security in an iterated process throughout that cycle. This poster introduces an authoritative reference model for DevSecOps, the Platform Independent Model (PIM).

Methods

We apply the PIM to supporting development and operation of network traffic analysis tools.

The DevSecOps Process builds cumulative information on the project in parallel with building the project itself. This cumulative information can be analyzed to identify threats to the project and to the DevSecOps process.

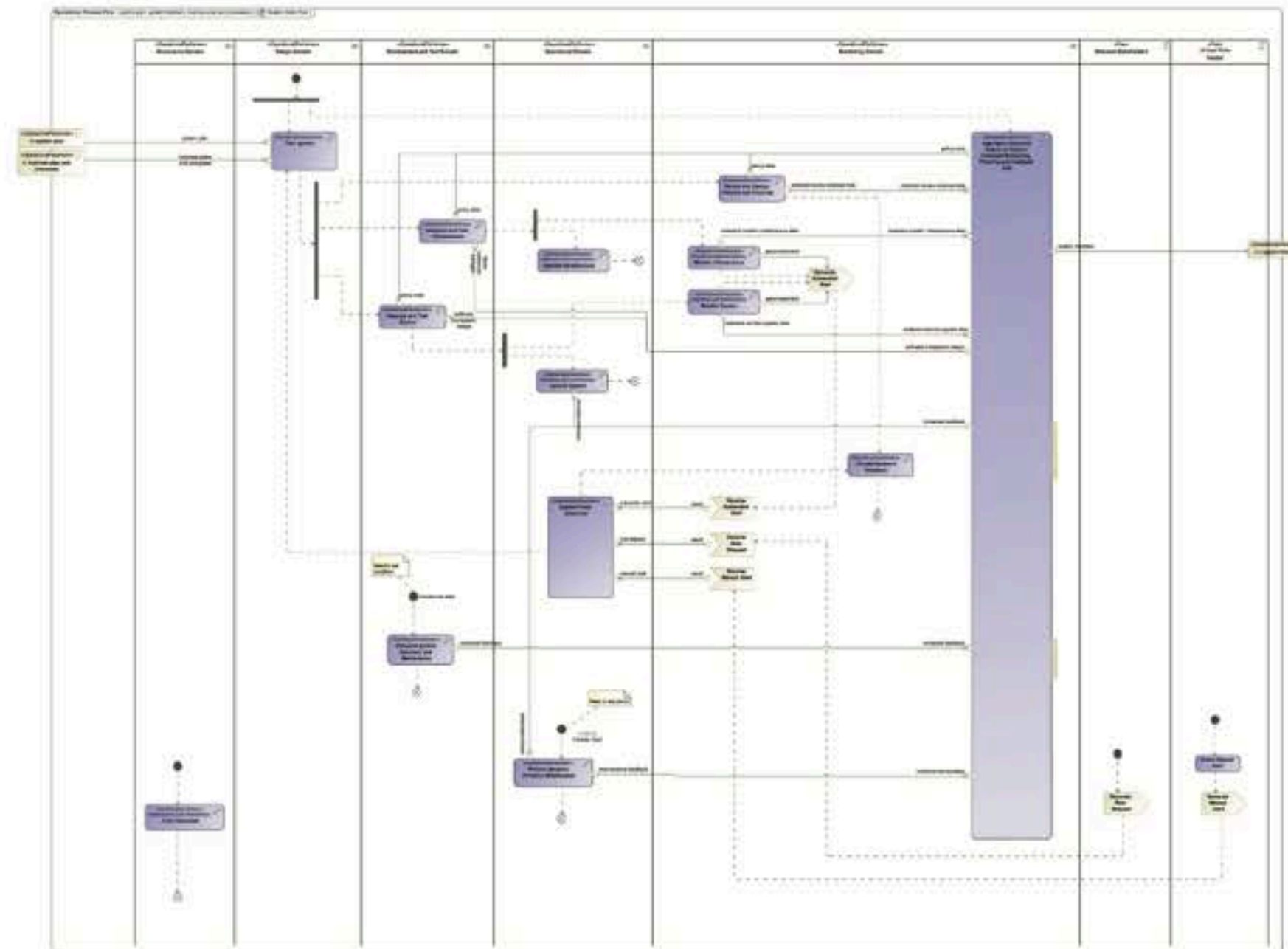
Discussion

The “plan system,” “integrate and test system,” and “operate system” activities can be configured to focus on network traffic analysis models, processes, and policies.

We incorporate network traffic analysis methods to address security concerns within the DevSecOps process including both observation of development logs and traffic information and evaluation of the products in operation.

Applying the SEI Platform Independent Model to support development and operation of network traffic analysis tools

<https://cmu-sei.github.io/DevSecOps-Model/>



Tables and Figures

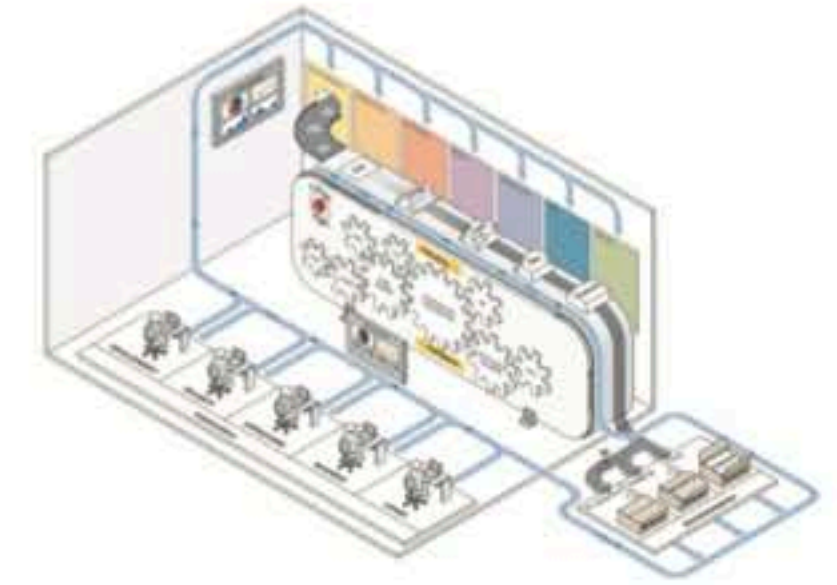


Figure 1: DevSecOps Pipeline

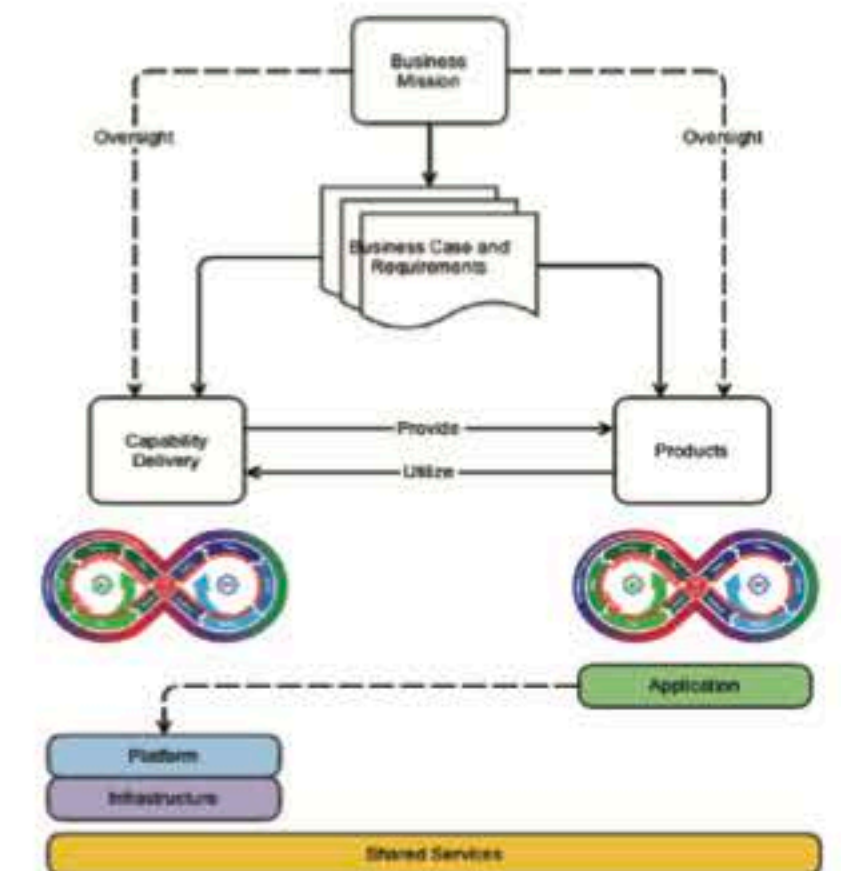


Figure 2: Integrated Pipeline and Infrastructure



Figure 3: Monitor Product Activity's Operational Process Flow