Centralized scan Factory for Application Security

Rohit Chouhan
Application Security Engineer
PepsiCo, TX, US
Email:rchouhan@cs.stonybrook.edu

Sera Kim
Application Security Engineer
PepsiCo, TX, US
Email:serakim1105@gmail.com

Chad Haley
Application Security Engineer
PepsiCo, TX, US
Email:chad.haley443@gmail.com

***Abstract*—**

message queues and on-demand containerized agents, the platform dynamically allocates compute resources for scanning tasks while maintaining centralized control, visibility, and reporting. This architecture ensures consistent scanning coverage with minimal manual intervention, optimizing both performance and cost efficiency.

1. Introduction

Application security in present day context is a domain encompassing static code scanning, API security, Edge security, container seurity, AI security, Web application firewalls. Modern applications ar sophisticated systems that consists of a large number of moving parts. Securing all of these is a daunting task, making modern AppSec a critical part of security for any organization. One key component of Application security is static source code scanning. Source code is what get builts as applications, hence it is important to identify and fix vulnerabilities in the source code.

Traditionally static source code scanning is done by using COTS scanners that can scan the source code for programming issues that can lead to vulnerabilities like SQL injection and cross-site scripting. These scanners also scan project dependencies like third-party libraries for known vulnerabilities in them, license issues. They also scan source code for hardcoded secrets.

Making effective use of these COTS scanners is a big challenge that organization face. Continuously scanning the source code and then surfacing the findings to the code owners is the main problem that any AppSec program has to solve. A popular approach folowwed by the a lot of organization is to put these scans in thier CI/CD pipelines. While this is a natural place for putting AppSec scans, the implementation of scans in CI/CD pipelines for a large organization is not easy or ideal. Coordinating with many devops teams to have the correct scans in correct places in all the pipelines i a difficult feat. Not only this but putting scans in the pipeline takes away the control, limits visibility, and required manual interventions to keep scans in a healthy running state. Tracking the findings from the scans and maintaining their history is another challenge that needs to be solved.

To address these challenges, we propose the Centralized AppSec Scan Factory, a cloud-native framework designed to automate, orchestrate, and scale application security scanning across enterprise repositories. The system integrates static application security testing (SAST), software composition analysis (SCA), and secrets detection into a unified pipeline. By leveraging event-driven orchestration through