Enterprise Application Security

State of Arizona – Department of Homeland Security

Project Investment Justification (PIJ #HL23003)

May 17, 2023

Agency Vision

To be the nationwide best practice for grant management and administration as well as a premier leader in cybersecurity among all state homeland security departments.

Agency Mission

Protect Arizona by providing strategic direction and access to resources that will enable all of the State's homeland security stakeholders to achieve our collective goals of: preventing terrorist attacks; enhancing border security; heightening cybersecurity efforts; reducing our vulnerability to all critical hazards; enhancing the capacity and expertise to plan for, mitigate, respond to and recover from all critical hazards that affect the safety, well-being, and economic security of Arizona; and building the resiliency of Arizona.

Team Introduction

Roles Present at ITAC

AZDOHS

- Ngan Pham - Statewide Cybersecurity Program Manager - AZDOHS

Veracode

- Matthew McIsaac - Manager Customer Success - Public Sector
- Max Hufft - Senior Solution Architect - SLED
- Jeff Fuson - Senior Account Executive - SLED
- James Salerno - Senior Customer Success Manager - Public Sector

Project Introduction

Stated Operational/Business Issue

- Budget Bill 2862 mandates the Department of Homeland Security to implement an enterprise license for:
    - Security software used by State Agencies
    - Integrate security into the development process
    - Scan software code in development, production, and post production
    - Detect and improve security threats by using at least two of the following:
        - Status Analysis
        - Dynamic Testing
        - Penetration Testing
        - Software composition Analysis
- The State currently lacks visibility and effective mitigation of security flaws in applications developed by its agencies and departments, increasing the risk of data breaches and other cybersecurity incidents.
- Application vulnerability assessments are periodically being conducted independently by agencies, but are not coordinated, and could miss coding flaws being introduced into mission critical business applications
- There is currently no enterprise solution for Application Security.

Project Introduction

Benefit to the State Agency and Constituents

- Identification of Application Security Risk across state agencies
- Single reporting platform from coding deficiencies to web application entry points
- Developer integration to ensure vulnerabilities are identified prior to production release
- Ability to decrease security debt in a timely manner with identification and resources
- Developer training on secure coding best practices
- Adheres to Cloud First Policy
- Provide Agencies with a means to comply with
    - STATEWIDE POLICY (8130): SYSTEM SECURITY ACQUISITION AND DEVELOPMENT

Proposed Solution

Overview of Proposed Solution

- SaaS based Application Security Platform
- Code Analysis, Software Composition Analysis, Web App + API Analysis
- Developer Training
  - eLearning - Video-based security training
  - Security Labs - Hands on developer training
- Ability to integrate into Developer Workstreams
- Security Consultant, Customer Success Manager/Engineer with PMP certification resources to ensure program rollout and understanding
- Single Platform to ensure continuity across agencies and overall governance reporting needs

Project Responsibilities

Identify Proposed Solutions Responsibilities

Agency

1. Integration
2. Scanning Cadence
3. Remediation
4. Introduce vendor to agencies

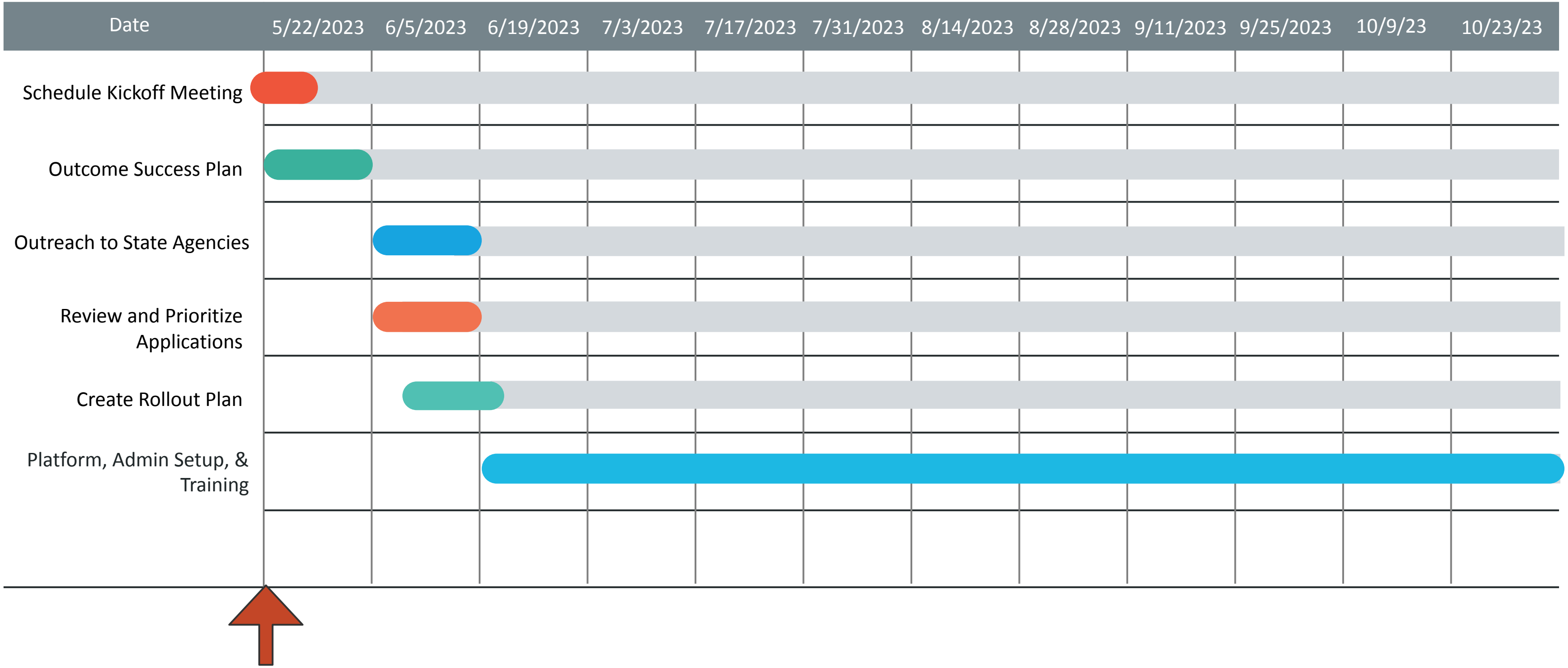
Shared

1. Training- Vendor supplied resources, Agencies must participate
2. Reporting Needs
3. Documentation - Vendor supplied, Agencies must read and engage
4. Project Planning
5. Reporting needs

Vendor/Contractor

1. Onboarding/Training of agencies
2. Generation of Reports
3. Program Management
4. Consulting Services
5. Provide technical resources
6. Supports platform

Project Timeline



Project Costs

ARIZONA
DEPARTMENT OF ADMINISTRATION
TECHNOLOGY

Project Costs by Category	FY23	FY24	FY25	FY26	FY27	Total
Professional & Outside Services (Contractors)						
Hardware						
Software						
Communications						
Facilities						
License & Maintenance Fees	1,741,512.52	1,741,512.52	1,741,512.52	1,741,512.52	1,741,512.52	8,707,652.60
Other Operational Expenditures						
Total Development	1,741,512.52					1,741,512.52
Total Operational		1,741,512.52	1,741,512.52	1,741,512.52	1,741,512.52	6,966,050.08

Financial Impact

ARIZONA
DEPARTMENT OF ADMINISTRATION
TECHNOLOGY

Breakdown of Financial Impact

Project Development Funding	
Base Budget - Available	1,741,512.52
Base Budget - To Be Requested	2,000,000
APF Budget - Available	
APF Budget - To Be Requested	
Other Appropriated - Available	
Other Appropriated - To Be Requested	
Federal - Available	
Federal - To Be Requested	

Total Development Project Funding	
Available Budget	1,741,512.52
To Be Requested Budget	0.00

Operational	
Current 3-Year Operational Cost (Avg)	5,224,534.56
Proposed 3-Year Operational Cost (Avg)	6,000,000
Financial Impact of New System	

Total Operational Funding - Project	
To Be Requested Budget	6,000,000

What Success Looks Like

Measures of Success

A. Within 6 months of procuring the application, 50% of **participating** agencies will have a minimum of one application scanned, one URL scanned, and one developer participating in the eLearning/lab platform.

B. Within 1 year, 100% of **participating** agencies engaged with the solution will have a minimum of one application scanned, one URL scanned, and one developer using the eLearning/lab platform.

Q & A
Session

Appendix

Proposed Solution

Due Diligence and Method of Procurement

ESPAC approved standing up an Application Security Product Evaluation Committee.

Five state agencies participated in the committee. Requirements were gathered. A Task Order was sent to all vendors on statewide contracts to bring forth their vendors/manufacturers to demo.

Each vendor were required to submit a completed requirements document, budgetary quote, and statement of work. Demos were conducted. Selection was based on the submitted documents and demo. Veracode will be purchased via an existing State Contract.

Technology

The Technology selected by was based on a technical requirements, functionality, ease of use, costs, and over impression.