ARIZONA
DEPARTMENT OF ADMINISTRATION
TECHNOLOGY

NASCIO 2024 State IT Recognition Awards
Cybersecurity

Statewide Application Security Enhancements

Description:	Improving and strengthening cybersecurity by scrutinizing software code to identify and address security threats
Contact:	Bryan Beach Bryan.Beach@azdoa.gov (602) 316-8369
Start date:	5/18/2023
End date:	12/22/2023

EXECUTIVE SUMMARY

The Arizona Department of Homeland Security (AZDOHS) has a mission to safeguard the state by providing strategic guidance and access to resources for all stakeholders. AZDOHS objectives are to prevent terrorist attacks, strengthen border security, bolster cybersecurity efforts, decrease Arizona's susceptibility to all critical hazards, improve the ability and know-how to prepare for, mitigate, respond to, and recover from any critical hazards that impact Arizona.

Situation

The potential risk posed by custom-developed applications in the state is not entirely clear. Although application vulnerability assessments are being conducted, there is a possibility that coding errors may be introduced into essential business applications and not be detected. AZDOHS is responsible for acquiring and implementing software that will integrate security measures into the development process and scrutinize software code during development, production, and post-production stages which will identify and address security threats.

Problems

The state is currently lacking visibility into custom-developed applications, and effective mitigation solutions of security flaws in applications developed by its agencies and departments. This increases the risk of data breaches and other cybersecurity incidents. While application vulnerability assessments are periodically being conducted by agencies that do them independently, hire contractors to do them, or are being provided by AZDOHS, these efforts are not fully coordinated and could result in coding flaws being introduced into mission critical business applications.

Solution

AZDOHS has been tasked with procuring and implementing an enterprise license for security software that will integrate security into the development process and scan software code in development, production, and postproduction to detect and reduce security risks by using at least two of the following testing mechanisms:

- Static analysis security testing
- Dynamic testing
- Penetration testing
- Software composition analysis

IDEA

AZDOHS will utilize the Veracode solution to integrate with development tools, ensuring consistent enforcement of security policies across state agencies. AZDOHS will have the ability to automate testing throughout the development lifecycle, facilitate application control audits at multiple points, and promote the development of more secure software. The solution will provide step-by-step guidance for understanding, prioritizing, and remedying vulnerabilities, help agencies adhere to web application security standards, and establish processes for consistently delivering secure software, thereby improving governance.

IMPLEMENTATION

AZDOHS was responsible for vendor management and procurement of the technology solution. The Enterprise Control Tower served as the product owner of this solution and provided support/assistance.

Individual state agency developers were responsible for their own application scanning, URL scanning, and participation in eLearning.

AZDOHS received quotes from three vendors (Microfocus, SHI, WWT) and selected the vendor WWT due to their ability to provide unlimited application scanning, unlimited developers to utilize the platform, and unlimited training.

IMPACT

In December 2023, AZDOHS implemented the solution to improve and strengthen cybersecurity by scrutinizing software code to identify and address security threats.

Veracode offers a full end-to-end application security platform and developer training, and is fully cloud native as a SaaS solution, maintaining alignment with P1100 - Cloud Smart Policy. It integrates application analysis into development pipelines, and provides multiple security analysis technologies on a single platform, including static analysis, dynamic analysis, and software composition analysis, to find security vulnerabilities such as malicious code and the absence of functionality that may lead to security breaches.