AppSecAI Expert Triage Automation

Benchmark Report

SAST Scanner: Commercial Product 1

Report Date: March 7, 2025

AppSecAI, Inc. Confidential

Executive Summary

Static Application Security Testing (SAST) tools are integral to identifying vulnerabilities. However, results must be manually triaged to remove false positives, a slow and expensive process that impedes application security, development and delivery. AppSecAI Expert Triage Automation (ETA) automates triage to lower manual triage time, tedium, and costs. This report evaluates AppSecAI and Commercial Product 1 against the open source OWASP benchmark with over 2,700 vulnerabilities. ETA analyzed a total of 11,598 findings in this assessment.

91.0%

Commercial Product 1 + AppSecAI Triage Accuracy

89.9%

Commercial Product 1 + AppSecAI True Positive Accuracy

5.6%

AppSecAI False Positive Rate

Metric	Commercial Product 1	Commercial Product 1 + AppSecAI
Accuracy	65.1%	91.0%
True Positive Accuracy	100.0%	94.7%
False Positive Rate	36.7%	5.6%
False Positive Findings	4,253	647

AppSecAI Benefit

84.8%

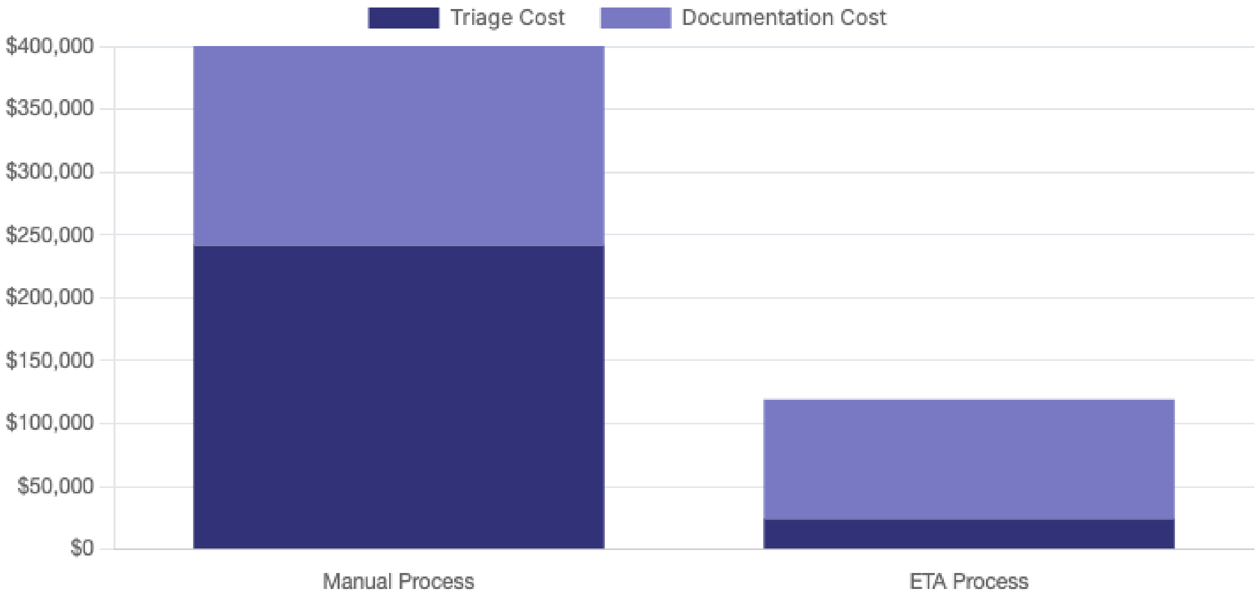
False Positive Reduction

3,606

False Positives Reduced

Financial Analysis

Cost Analysis Summary: Implementation of Commercial Product 1 + AppSecAI demonstrates significant cost savings across all security assessment processes. The total cost reduction is $280,795.833 (70.2%), with notable improvements in both triage and documentation costs. This substantial decrease in operational expenses enables security teams to process vulnerability assessments more efficiently while maintaining high accuracy.



Cost Rates

Developer Cost: $175/hour

AppSec Analyst Cost: $250/hour

Time Metrics

Manual Triage: 5 min/vuln

Documentation: 5 min/vuln

ETA Triage: 0.5 min/vuln

Appendix: Glossary of Terms

This glossary provides definitions for key terms used throughout the report to ensure clear understanding of the report metrics.

AppSecAI ETA (Expert Triage Automation)

An AI-powered solution that automates and accelerates vulnerability triage by removing false positives and documenting true positives.

Triage

The process of reviewing, categorizing, and prioritizing security findings to determine their validity and impact.

Accuracy

The percentage of findings that are reported correctly (whether in the OWASP Benchmark or not).

True Positives

Real Vulnerabilities (whether in the OWASP Benchmark or not) that were reported as vulnerable.

False Positives

Not Vulnerable Test Cases (whether in the OWASP Benchmark or not) that were reported as vulnerable.

True Negatives

Not Vulnerable Test Cases in the OWASP Benchmark that were also not Reported by the SAST Tool.

False Negatives

Not Vulnerable Test Cases (whether in the OWASP Benchmark or not) that were reported as vulnerable by the SAST tool.