opentext™ | Cybersecurity

Position Paper

Increase Speed and Accuracy with AI Driven Static Analysis Auditing

Leveling up Fortify's Audit Assistant AI

Triaging and validating raw static analysis results is one of the most time-intensive manual processes within application security testing. Fortify Audit Assistant leverages past audit decisions to power machine learning-assisted auditing, validating results immediately and dramatically reducing manual auditing efforts and excess noise in scan results. The next-generation models for Fortify Audit Assistant level up the accuracy, performance, and power even further.

Machine Learning for Auditing

Fortify's application security as a service offering Fortify on Demand by OpenText runs thousands of static, dynamic, and mobile scans per week, scanning billions of lines of code. Fortify on Demand takes customer application source code, runs the scan, then (as a value added service) passes these raw scan results to a team of expert auditors who are subject matter experts. These auditors identify and prioritize the noteworthy findings while removing the noise from the results. Consequently, Fortify on Demand customers receive actionable results and can primarily focus on fixing the most critical issues.

The Fortify Audit Assistant by OpenText service uses machine learning algorithms to feed off the hundreds of millions of anonymous audit decisions from Fortify on Demand experts. These decision models are actively used and developed for Fortify on Demand, but are also technologies that can be automatically applied on-prem to Fortify Static Code Analyzer by OpenText results by using Audit Assistant. This innovative and patent-pending technology has been made available to Fortify customers for the past five years.

The Fortify Audit Assistant service uses machine learning algorithms from hundreds of millions of anonymous audit decisions. These decision models can be automatically applied to Fortify Static Code Analyzer by OpenText results by using Audit Assistant.

Leveling up the AI

Interset is the division of OpenText™ Cybersecurity that specializes in artificial intelligence and machine learning. Interset has partnered with the Fortify division to level up the models that power the Fortify Audit Assistant (AA) service.

Account for Model Drift

Model drift is a statistical phenomenon where, as the world changes, initially effective models may have new opportunities to improve. Cybersecurity does not stand still: novel attacks and vulnerabilities appear all the time, and new countermeasures and detections respond in kind.

The new AA models provide a way to refresh the approach and address any model drift that may have happened since the technology was first pioneered, along with designing for a learning pipeline that will be more resilient to drift going forward.

Incorporate Additional Data and Context

Key to accurate machine learning is always data: the more available data, the more contextual clues are afforded to the AI to learn from. The more granular the target to predict, the more effective and precise the trained models can become.

The new AA models take in additional anonymized vulnerability metadata about the scans that allow them to be more predictive than ever before. In addition, while the original models predicted a binary value (e.g., false positive or not), the new models support more granular category labels than before (e.g., False Positive, Exploitable, Suspicious, Mitigated).

More Flexibility to Learn from Your Unique Environment
AA models learn as a prerequisite from all of the expert human auditors and language experts on Fortify on Demand's audit team—an incredible resource that is unparalleled in this industry. However, we recognize that every customer is different, every project is different.

We designed the new AA model pipeline to also learn the unique behaviors in your projects. This learning gets better and better over time; the more you audit your vulnerabilities, the more the models learn about what's appropriate for your project—all while remaining sensitive to your IP, using anonymized vulnerability metadata, and without operating on the source code itself.

Audit Assistant gets better and better over time. The more you audit your vulnerabilities, the more the models learn about what's appropriate for your project.

Design and Testing Methodology

Like software engineering, effective data science demands a disciplined approach to model development. The Interset and Fortify data science teams started by testing the existing models to measure their strengths and weaknesses.

We also interviewed and worked with the Fortify on Demand audit teams to better understand how they applied their language and security expertise to perform their audits. We worked with the Fortify on Demand engineering teams to use real-world, anonymized production data for our training and testing. Finally, we performed exploratory data analyses and feature engineering to develop the new models on the latest data.

We performed model testing and validation on actual data from Fortify on Demand, over the course of 20-weeks. Because AA models forecast into the future, we performed all model validation using proper back-testing approaches (i.e., training on past data, comparing results against future data).

As we deploy these new AA models into production, the mechanisms to validate and measure their performance happens continuously and automatically.

Results of Our Testing

Accuracy
The new models show strong accuracy performance. In our testing using 20-weeks of real-world data from our production Fortify-on-Demand systems, our new models were 60% more accurate, on average, for predictions compared to the previous generation's models. In particular, the JavaScript, Java, and HTML models demonstrated great improvements.

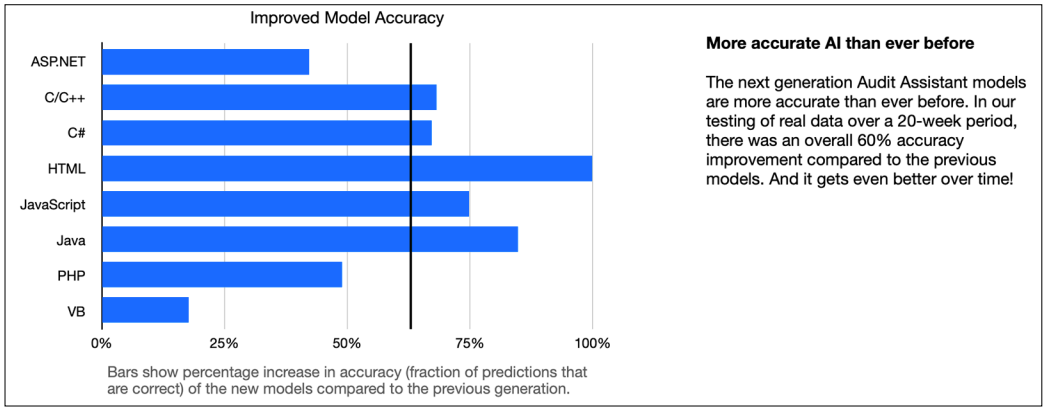

Figure 1. Improved Model Accuracy

Recall

When measuring the performance of machine learning models, it is important to not only focus on how many predictions the models got *right*, but also how many items were *detected*. This is measured through something called 'recall,' which is the percentage of issues correctly identified. A high recall score means fewer false negatives and that little slips through the cracks.

The new AA models show an average recall of nearly 80% in our testing, which is excellent.

Also, while the previous models were binary classifiers (False Positive or not), the new AA models are multi-class predictors that learn to predict all the observed category labels. This additional granularity is helpful if your organization uses custom category labels beyond the standard default set.

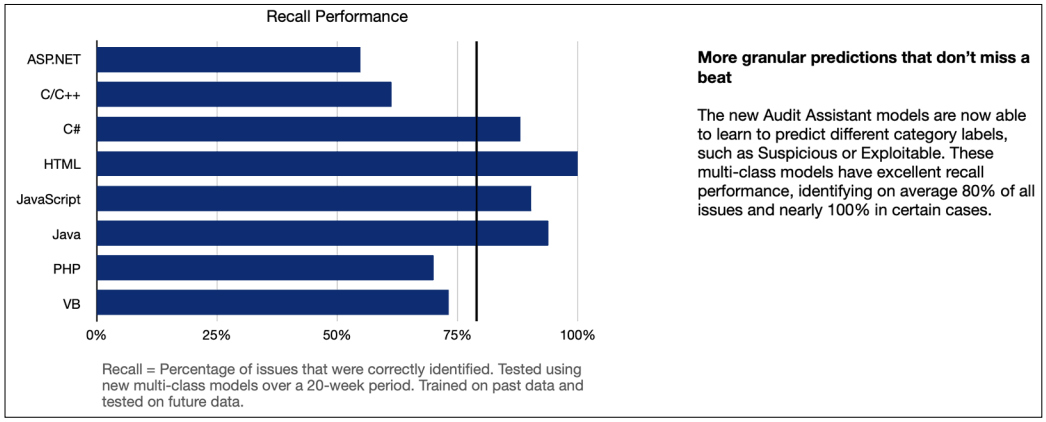

Figure 2. Recall Performance

Accuracy over Time

As machine learning models continue to consume more training data over time, they become more accurate. The new AA model pipeline balances recent and past data; recent behaviors are weighted more highly than distant past behaviors. Further, there is also a balance between the global model (trained on the Fortify on Demand data that represents aggregate learning across many customers of the FoD audit service) and the local model (behaviors that are unique to your organization and project).

These new features help address model drift while ensuring that models get better, not worse, over time.

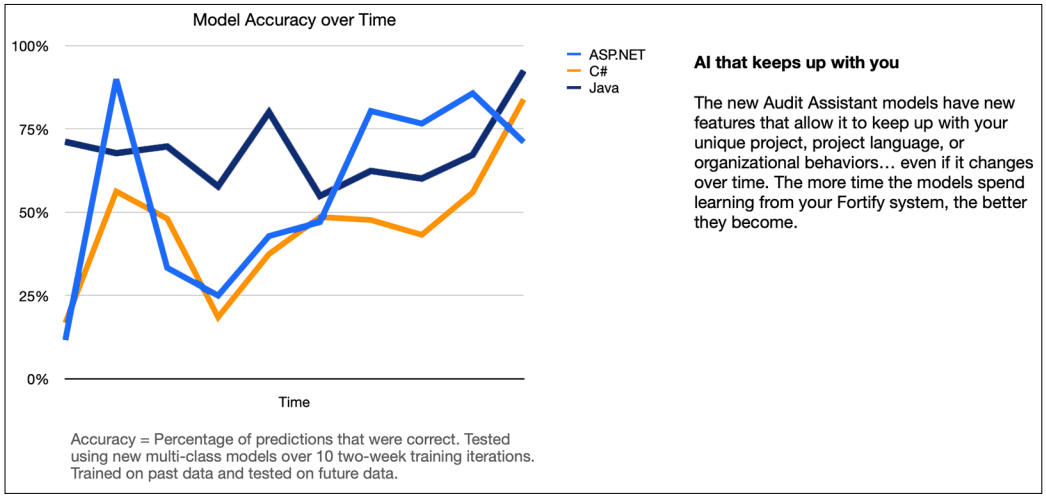

Figure 3. Model Accuracy over Time

Conclusion

Auditing raw static scan results is the most time-consuming and effort-intensive manual aspect of SAST and requires a skillset that is often difficult to find and keep.

The initial release of Fortify Audit Assistant was ground-breaking and an industry first. This capability uses machine learning to democratize the Fortify on Demand human audit team's expertise to help close the skills shortage in performing effective audits.

Now, five years later, the next generation of models for Fortify Audit Assistant make the AI more effective than ever before. We can't wait to get these next generational models into your hands.

Learn More

- Audit Assistant Web Page
- Audit Assistant Datasheet

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.