opentext™ | Cybersecurity

Position Paper

OpenText Security Fortify Audit Assistant

Table of Contents

Introduction

Introducing machine-learning–assisted auditing of Fortify Static Code Analyzer (SCA) by OpenText™ results. Security Fortify now unlocks and reproduces contextual awareness and security expertise from Fortify SCA results for the first time in the history of application security testing.

Why We Did It

A fundamental problem with static code analysis has always been that it requires human auditing before the results are actionable. The action of auditing is a leading segment of non-value–added time.

What's the Value?

- Reduces the number of issues that need deep manual examination
- Identify relevant issues earlier in the SDLC
- Scale application security with existing resources
- Maintain consistency in auditing and reporting
- Increased ROI on existing Fortify products

Why Static Application Security Testing?

Static Application Security Testing (SAST) is the market of products and services that analyze an application's source code, bytecode, or binary code for security vulnerabilities as defined by Gartner.[1] The National Institute of Standards and Technology (NIST) notes that static analysis tools are one of the last lines of defense to eliminate software security vulnerabilities during development or after deployment.[2] These software security tools and services report weaknesses in source code that can lead to vulnerabilities an adversary could exploit, to the detriment of the enterprise. If source code implements weak security, the business is exposed to additional risk that is unknown without SAST. Static application security testing enables enterprises to know their risk, transform their security posture, and make informed decisions to protect the business.

Software vulnerabilities are a serious problem introduced by mistake, through poor software security practices, or intentionally by internal threat actors. The software development process is often not controlled to minimize these vulnerabilities. Static analysis provides the enterprise with the intelligence necessary to identify, monitor, and reduce the business risk from an application's source code and provides recommendations to remediate issues. Static code analysis has been widely recognized as a necessary component of securing the digital enterprise for nearly two decades. As the President's Information Technology Advisory Council noted in a 1999 report, software development methods that have been the norm fail to provide the high-quality, reliable, and secure software that the IT infrastructure requires.[3]

1. Gartner Magic Quadrant for Application Security Testing 2015. **www.community.hpe.com/t5/Protect-Your-Assets/HP-Fortify-The-Undisputed-Leader-in-2015-Gartner-Magic-Quadrant/ba-p/6776163#.WC5FZrIrKM8**
2. NIST Source Code Security Analyzers. **www.samate.nist.gov/index.php/Source_Code_Security_Analyzers.html**
3. NITRD 2005 President's Information Technology Advisory Council. **www.nitrd.gov/Pitac/Reports/20050301_cybersecurity/cybersecurity.pdf**

Confirmation of Software Vulnerabilities

SAST reports categorize issues by their criticality. Issues must then be manually confirmed as exploitable, or marked as not an issue by expert application security auditors. There are many reasons underlying a determination of not an issue. While some findings are false positives, more often the finding is not relevant because of organizational policy, or is not exploitable due to mitigations being in place, or the potentially vulnerable code being unreachable.

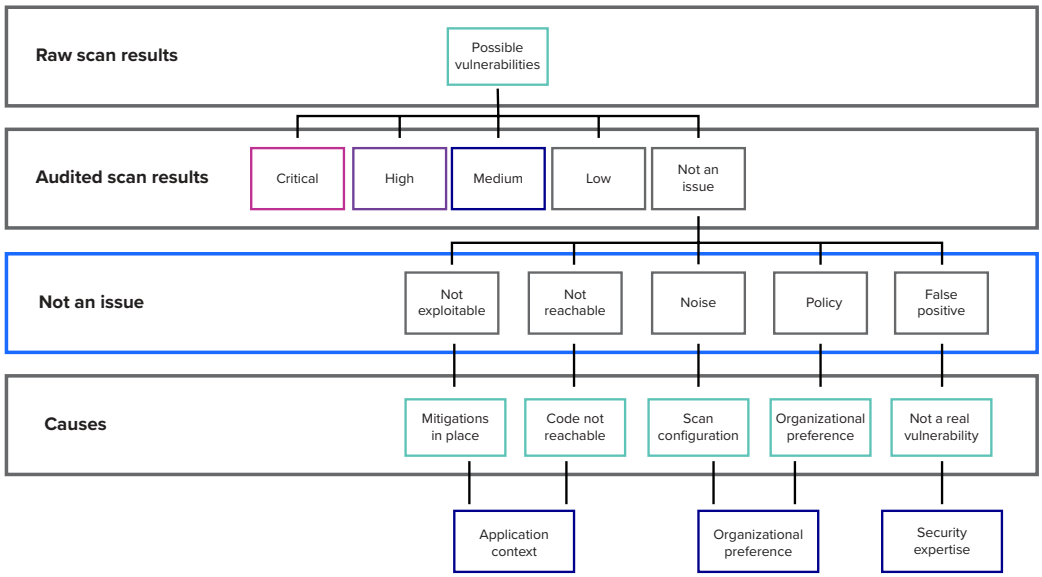

Figure 1. Scan finding classification

SAST tools report findings of potential vulnerabilities in an application by using different analysis methods such as taint, structure, or control flow analysis. Expert auditors are required to validate findings using details specific to their enterprise, such as the context of the application and deployment. When auditors determine a potential software security vulnerability is not an issue, the time spent on verification is non-value added time. These time-consuming audits have traditionally come at significant cost to the enterprise and expose a fundamental challenge with delivering secure applications; tools and technology do not immediately produce actionable intelligence.

The well-recognized cybersecurity skills gap[4] adds to the challenge of software security assurance. Skilled security professionals rightfully command high salaries, and by definition,

4. CSO Online. **www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html**

even the best individual contributors cannot be effectively scaled to the enterprise's needs. Static analysis tools make the impossible job of securing code possible, and a skilled auditor's software security expertise verifies actionable findings. Even the best security teams are ultimately limited by the human experience available, which often pales in comparison to the universe of potential software flaws to which the organization is exposed. The next evolution of secure applications comes by leveraging machine learning to make the process of securing developing applications quick and efficient. These techniques extend the reach and better scale the expertise of the security professionals through the security development lifecycle.

Machine-Learning and Predictive Analytics: the Next Generation of SAST

The actionable intelligence problem is addressed through the Security Fortify scan analytics platform. Fortify has been deploying and validating this approach with Fortify on Demand by OpenText for over a year, and has been delivering monumental improvement to the issue auditing process. This capability is now available to on-premises customers of Fortify Software Security Center by OpenText via its Fortify Audit Assistant by OpenText feature. Fortify Audit Assistant identifies relevant exploitable vulnerabilities specific to your organization, in new static scan results. It does this by employing scan analytics machine-learning classifiers that are trained using anonymous metadata from scan results, previously audited by software security experts. The scan analytics platform delivers this capability as a web service in the cloud, enriching SCA scan results with audit predictions with up to 98 percent accuracy.

Fortify Audit Assistant enables machine-learning assisted auditing and leverages the security expertise of the entire Security Fortify community without transmitting any sensitive information. Fortify Audit Assistant transmits only anonymized metadata derived from the scan results called anonymous issue metrics. Neither scan results nor code ever leaves the SSC environment. Issues indicated by the proven Fortify Static Code Analyzer are parsed by Fortify Audit Assistant into non-sensitive attributes. These attributes include vulnerability category, severity, and measures of code and software security vulnerability complexity—such as the number of inputs, branches, method output types, programming language, f/ile extension, and the analyzer that found the issue. In the case of training data, the auditor's previous determination is also included. The anonymized issue metrics are sent to Fortify scan analytics to train and apply machine-learning classifiers, which identify issues with up to 98 percent accuracy.

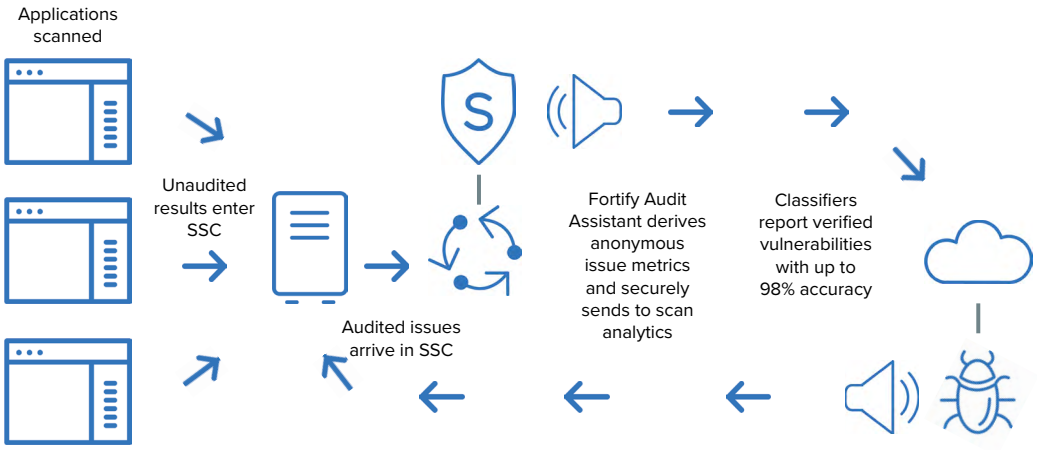

Figure 2. Fortify Audit Assistant workflow

After processing a new static scan result, audit assistant will add its prediction and prediction confidence to the scan results. Based on an organization's risk tolerance and preconfigured confidence thresholds, those issues will then be categorized as Exploitable, Indeterminate, or Not an Issue.

- The prediction value indicates whether Fortify Audit Assistant considers the issue Exploitable, Not an Issue, or if the prediction confidence falls below the threshold, Indeterminate.
- The prediction confidence represents the confidence audit assistant has in the accuracy of its prediction.

Without exposing sensitive or identifying information, Fortify Audit Assistant determinations are added back to the scan results and made available for review by an organization's security auditors. Anonymized metadata remains protected in the TLS encrypted communication channel throughout its transmission through the cloud. Transmitting only the anonymous issue metrics allows the enterprise to scale its software security assurance program and decrease its risk while not allowing sensitive data outside of its normal protections.

By deriving issue metrics from the customer scan results, audit assistant empowers the enterprise to leverage the knowledge of thousands of security professionals who have collectively evaluated billions of lines of code. Without expanding headcount or allocating additional budget, the enterprise's application security program becomes more efficient and effective through machine learning. This paradigm shift in SAST from scarce human expertise to the limitless scalability of artificial intelligence reduces non-issue findings by up to 90 percent.

What is a non-issue?

A non-issue is a finding that has been audited and does not require remediation. Non-issues can be caused by:

- The issue was not exploitable due to remediation efforts already in place
- Code is unreachable by design
- Noise caused by poor tool configuration
- An organizational decision to accept the risk
- A false positive

Non-issue reduction:	**25%–90%**
Accuracy:	**80%–98%**
False negative:	**<1%**

Drastically Increase Return on Investment

Measures of the return on investment (ROI) from new SAST implementations have been readily available for years.[5] The enterprise reaps significant savings through reduced remediation costs from shifting left in the software security lifecycle and avoiding breeches via improved application security. Fortify Audit Assistant is poised to maximize returns on existing investments and help the organization shift-left[6] by drastically reducing the audit and issue remediation time after a scan is complete. Through machine-learning techniques, Fortify Audit Assistant extends the reach of scarce security expertise. Expert's time is optimized by classifiers learning from thousands of security professionals across the whole Fortify community. Software security assurance programs can scale to the whole enterprise while ensuring accuracy and consistency.

Vendors have made tradeoffs between the noise and potential false negatives that worry every security professional. Fortify Audit Assistant reduces the noise by up to 90 percent while simultaneously keeping false negative classifications to below one percent. Fortify Audit Assistant classifiers correctly audit Fortify SCA findings as non-issues with up to 98 percent accuracy. The accuracy of scan analytics classifiers is improved through training data supplied in one of two ways:

- **Fortify community intelligence**
  The classifier is trained using Fortify community intelligence, leveraging the expertise of Fortify on Demand auditors, dedicated software security researchers, and other Fortify customers participating in the community intelligence. Users opt in to including only their anonymous issue metrics into the Fortify community intelligence data set, which improves the quality of the predictions for all users. Classifiers trained with Fortify Community Intelligence in addition to a customer's local data are the most accurate and robust, containing the latest information on rules and zero days. In addition, classifiers trained on the Fortify Community Intelligence can be utilized out-of-the-box to predict accurately without requiring customers to submit training data.

5. Does Application Security Pay? Measuring the Business Impact of Software Security Assurance Solutions. **www.software.microfocus.com/software/fortifyroi**
6. Integrate application security into your DevOps program. **https://files.asset.microfocus.com/4aa6-3394/en/4aa6-3394.pdf**

- **Private intelligence**
  Classifiers are trained only on a customer's anonymous issue metrics derived from historical audited scan results. Prior to predicting on new scan results, historical scan results are parsed and submitted to Fortify Audit Assistant for training. An organization's anonymous issue metrics are not available for training by others.

? How is customer data secured?

Issue metrics are calculated locally and anonymized so as to never be identifiable outside of the Fortify Software Security Center instance in which it lives. Security controls include:

- Local derivation of issue metrics
- Issue metrics contain no sensitive information
- Obfuscation by prediction request ID
- End-to-end encryption

Regardless whether the user opts into the Fortify Community Intelligence or chooses to train classifiers only with their own private data, customers can rest assured that issue metrics are derived and anonymized locally. Security Fortify focuses solely on security, using our expertise to solve yesterday's security problems while delivering tomorrow's security capabilities.

Security Risk

Static analysis produces issue data that informs the business of its exposure through the application layer. Issue data that is identifiable outside of the enterprise is a roadmap for breach, so issue data never leaves the enterprise with Fortify Audit Assistant. Issue data is anonymized locally before transition so it cannot be used to discover issues or their location.

Fortify Audit Assistant contacts the scan analytics service for predictions asynchronously so it cannot block the progression of the auditing and remediation process. If scan analytics service becomes unavailable for any reason, the workflow continues without Fortify Audit Assistant predictions. Once the service is available, predictions begin to flow again.
The enterprise's risk is lowered by employing Fortify Audit Assistant as part of the secure software development lifecycle due to the thousands of security expert reviews used to train classifiers. Local security experts are then free to triage and prioritize more critical and questionable findings for the enterprise.

Accuracy

Fortify Audit Assistant is only as accurate as the data it is trained on. If an audited issue is right 50 percent of the time in the issue metrics used for training a classifier, that classifier will be right 50 percent of the time as well. Thus, classifiers trained with the Fortify Community Intelligence are more accurate and consistent because they contain the combined expertise from millions of training records from world-class security professionals. Classifiers trained with the Fortify Community Intelligence have been measured as having 98 percent accuracy. Opting in to including anonymous issue metrics into the Fortify Community Intelligence allows

the enterprise to benefit from the combined security knowledge and domain expertise of the proven security experts across Fortify and its community with their own security professionals to boost that 98 percent accuracy higher for all users.

A given organization may have the greatest experts on the planet for locating and remediating SQL Injection vulnerabilities from one framework, but enterprise code may span multiple frameworks and languages. By opting in to Fortify Community Intelligence, the best expertise is available from specialists in all supported languages and frameworks. The accuracy of classifiers is improved through sourcing expertise for continuous training. An enterprise can benefit from the existing high level of accuracy present in public classifiers while contributing to their improvement with their own internal expertise.

Conclusion

This paradigm shift in static analysis dramatically increases return on investment as the time and cost to audit results decrease substantially. Enterprises now have the capability to leverage the knowledge of thousands of security professionals who have collectively evaluated billions of lines of code within their own software assurance programs through Fortify Audit Assistant. Rather than reduce the breadth of security issues through limiting what analyzers report, Security Fortify has created the scan analytics platform to distinguish non-issues from real issues automatically. This innovative approach utilizes Big Data analytics to scale secure software assurance to the enterprise without sacrificing scan depth or integrity.

As organizations transition to a DevOps environment, application security must be built into their processes. Security Fortify Audit Assistant directly helps automate the auditing process so deliverable and deployment schedules are met. Fortify Audit Assistant uniquely reduces the repetitive, time-consuming work of issue review through the scan analytics platform. Enterprises no longer need to accept noisy scan results, make tradeoffs between scan comprehensiveness and time-to-audit, or negatively impact product delivery dates with scan review time. Classifiers trained on anonymous issue metrics reduce the expense of software security assurance programs without the risk of identifiable data transmitted to the cloud. Organizations immediately reduce their overall security workload through vulnerability prediction by opting in to use the Fortify product line's community intelligence classifiers.

Security Fortify was founded in 2003 and has been providing the industry-leading Fortify Static Code Analyzer (SCA) tool for a scientifically sound approach to secure software development that enables meaningful and practical testing for consistency of specifications and implementations for more than a decade.

Learn more at
www.microfocus.com/en-us/solutions/application-security

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.