VERACODE

Veracode SecurityInsights

Key Facts

SecurityInsights Highlights:

- Industry's first complete application intelligence and data analytics service
- Allows C-Suite Execs to set objectives for security quality and application risk using actual code-level metrics
- Informs acceptance criteria in contract negotiations with 3rd parties
- Delivered as a simple and easy to use cloud-based service
- Aggregates statistics from growing database of thousands of applications and billions of lines of code
- Covers findings from multiple testing techniques – static, dynamic, manual
- Covers entire software supply chain – Internally developed, Commercial, Open Source and Outsourced
- Covers web and non-web applications across broad set of languages and platforms including Java, .Net, C/C++
- Powerful 'Compare Me' capability to allow performance benchmarking against industry standards and peer group
- Awarded CSO Magazine's Emerging Solutions Demo Award

2010 EMERGING SOLUTIONS DEMO AWARD

SecurityInsights is a first-of-its-kind application intelligence service. It empowers customers with the code-level security information needed to make informed application risk management decisions across the entire software supply chain. With SecurityInsights, executives and security professionals can set peer-based or industry-based benchmarks for security quality of internally developed software, establish appropriate third-party purchase and acceptance criteria, and address increasingly thorough audit or compliance requirements.

The Case for Application Intelligence

Software applications are the enterprise's new security perimeter. Today's applications control access to financial data, public service infrastructure, patient health records, personal information on mobile devices and more. Their weaknesses have become the target of most new attacks. Exploited vulnerabilities such as backdoors, malicious code, and Zero-day flaws have had expensive and embarrassing consequences.

We conceptually know that applications are vulnerable. However, real information and meaningful metrics are needed about why software remains so insecure and what can be done to improve the status quo. If a CISO knew that between 30 and 70 percent of all code in what they thought of as internally developed applications was identifiably from third-parties, how would that inform their approach to vendor and third-party risk management? If a VP of Engineering was equipped with hard facts to dispel the fear surrounding use of open source software, how would that impact the software architecture and cost of building new products? If there was a way to compare the state of an enterprises' software security vs. peers in the industry, how would that help build the case for appropriate funds allocation for an enterprise's application risk management program?

The SecurityInsights Difference

Until now most of the information available has come from "perimeter defense" companies that provide network, gateway or endpoint protection technologies such as firewalls and anti-virus. While valuable, these approaches are insufficient because they focus on known vulnerabilities and not the all-important unknown or Zero Day vulnerabilities that are hidden in the final application binary and subject to attack by sophisticated hackers. Other reports, such as those from website security testing companies, typically represent only one type of testing ("black box" or "dynamic") performed against a single type of application (web applications). Missing until now has been security intelligence derived from multiple testing methodologies (static, dynamic, and manual) on the full spectrum of application types (components, shared libraries, web and non-web applications) and programming languages (including Java, C/C++, and .NET) from every part of the software supply chain (Internally Developed, Open Source, Outsourced, Commercial). By filling this void Veracode's SecurityInsights cloud-based service brings clarity and a broader perspective into the security quality produced by the complex global software supply chain and what it means for you.

VERACODE

"Having the ability to compare the state of security in our application portfolio to other organizations in similar industries and projects across Veracode's comprehensive repository of applications from around the world will be invaluable. This information at our fingertips will not only help us make the right business decisions, but will enable us to see where we can improve before a problem arises."

Donna Durkin, chief information security and privacy officer, Computershare.

Computershare

For More Information:

For information on software security services, best practices, and methodologies, contact us at.

Veracode, Inc.

4 Van De Graaff Drive

Burlington, MA 01803

Tel: +781.425.6040

Fax: +781.425.6039

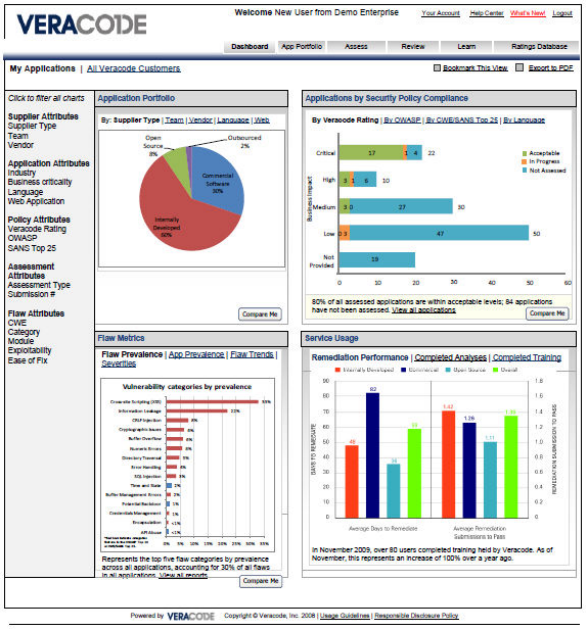
URL: http://www.veracode.com

How it Works

Customers access SecurityInsights by logging into Veracode's cloud-based application risk management services platform. The data analytics capability built into the platform allows customers to explore many different dimensions of the state of software security including but not limited to:

- **Application Profile and Portfolio Distribution:** Provides a view into the distribution of languages, platforms and supplier types that form modern enterprise application portfolios.
- **Application Security Policy Compliance:** Benchmarks security quality and compliance against risk adjusted enterprise security policies.
- **Vulnerability Distribution and Prevalence:** Enumerates the top vulnerability categories by language, platform and supplier types. Can be used to determine vulnerability categories particularly prevalent in a certain language family such as C/C++ or absent from a class of software such as open source software.
- **Industry Standards Compliance:** Depicts performance againstindustry standards such as SANS Top 25 or OWASP Top 10.
- **Remediation Performance:** Provides information on number of submissions and timeline to achieve compliance with security policies designated for applications of differing business criticatliy.

All of the above application intelligence categories allow further exploration and filtering of data by industry, supplier type, language etc.



Compare Me

For customers that subscribe to both SecurityReview and SecurityInsights a "Compare Me" capability is available that allows instant side by side comparison their software portfolio with the aggregated security quality benchmarks from thousands of applications for their industry, programming language and software supplier type. For example, an enterprise can see what percentage of their applications comply with SANS Top 25 vs. all applications in their industry peer group. Even granular comparisons such as Top vulnerabilities present in their Java applications vs. Java applications across the entire database can be made. This allows for setting of appropriate improvement and training and education goals.