Press Release

Code Dx Enterprise 3.0 Now Offers Static and Dynamic Hybrid Analysis for Application Security Testing

The Software Vulnerability Correlation and Management Solution also Further Expands Support for AppSec Tools, Including ESLint and Cigital Cedar

SAN FRANCISCO, CA and NORTHPORT, N.Y.—April 16, 2018—(**RSA Conference 2018**, Booths #ESE-07 and DHS S&T #1839 South)—**Code Dx, Inc.**, provider of an award-winning application security solution that automates and accelerates the discovery, prioritization, and management of software vulnerabilities, today announced a significant new capability— Static & Dynamic Hybrid Analysis—to be included in Code Dx Enterprise 3.0, its flagship Application Software Vulnerability Correlation and Management solution.

Hybrid Analysis combines the best aspects of the two most common types of application security testing—static application security testing (SAST) and dynamic application security testing (DAST)—to provide a deeper, more effective security analysis of a Java application. SAST tools scour the source code for potential vulnerabilities—from the inside out—while DAST tools dynamically "attack" running applications, from the outside in, to find exploits that are accessible to an attacker. In isolation these approaches provide information that is not **immediately actionable**, or that is otherwise difficult to prioritize. The Code Dx Hybrid Analysis capability combines the inside-out and outside-in approaches to shine a spotlight onto vulnerabilities that both **exist** in the code and are also shown to be **exploitable**—immediately confirming a potential weakness as a true, genuine threat. This yields information developers need to decide how to best, and most quickly, secure the application.

"The perspectives and techniques used by SAST and DAST tools are very different," said **Anita D'Amico, Ph.D.,** CEO of Code Dx. "Being able to combine the inside-out approach of SAST tools with the outside-in approach of DAST tools lets users easily and affordably improve their analysis speed, accuracy, and confidence in detection of vulnerabilities by cross-mapping and normalizing the output of hybrid techniques."

In addition to Hybrid Analysis, Code Dx Enterprise 3.0 supports and integrates with more than 40 commercial and open-source SAST, DAST, and IAST tools and techniques to provide total software application vulnerability correlation and management. New to Version 3.0 are several new tools, including:

- **ESLint**—software quality assurance and security tool for JavaScript, JSX, and NodeJS applications.
- **Cigital Cedar**—on-demand penetration testing tool.

About Code Dx

Code Dx, Inc. is a provider of an award-winning application security solution that automates and accelerates the discovery, prioritization, and management of software vulnerabilities. The Code Dx Enterprise solution integrates the results of multiple static, dynamic, and interactive Application Security Testing (AST) tools, third-party component analyzers, threat modeling, and manual reviews into a consolidated set of results for quick and easy triage, prioritization, and remediation. The core technology was partially funded by Department of Homeland Security Science & Technology (DHS S&T) to help secure the nation's software supply chain. For more information, please visit **www.codedx.com** or contact Code Dx at (631) 759-3993 or at **Info@CodeDx.com.**

Press Inquiries:

Karen Higgins
A&E Communications, Inc.
610-831-5723
khiggins@aandecomm.com