SECURE DECISIONS
A DIVISION OF APPLIED VISIONS, INC.

PRESS RELEASE

Secure Decisions releases new technology to help streamline and enhance web application penetration testing

Northport, NY—January 31, 2019—Secure Decisions, a division of Applied Visions, Inc. and a recognized leader in cyber security, has developed a new application security testing technology, the ***Attack Surface Detector*** (ASD), that enhances and streamlines software penetration testing. Developed under the Department of Homeland Security Science and Technology Directorate's multi-year funded ASTAM (Application Security Technologies and Metrics) program, the ASD helps penetration testers by automating the discovery of a web application's hidden endpoints and optional parameters, and identifying gaps in an application's visible attack surface.

Automated penetration testing is a popular method to identify exploitable vulnerabilities in a web application, but often fails to identify unlinked endpoints and optional parameters, even with extensive brute force testing. This leaves untested gaps in an application's visible attack surface. Relying on manual penetration testing to identify testing gaps is an arduous, time consuming, and costly exercise. It does not guarantee complete identification of an application's attack surface, and consequently often leaves an application vulnerable, despite a pen tester's best effort to secure it from attacks.

The open source ***Attack Surface Detector*** plugin tool—available as both a standalone Command Line Interface tool and as plugins for the widely-adopted Burp Suite (from Portswigger) and OWASP ZAP Dynamic Application Securing Testing (DAST) tools, helps solve this problem. The Attack Surface Detector was developed to provide a complete picture of a web application's exposed attack surface. It automatically examines an application's source code via static analysis, finding hidden or unlinked endpoints and identifying their optional parameters and data types that are often missed by most DAST scanners. This greatly accelerates the attack surface identification process, saving substantial time for manual penetration testers. These discovered endpoints and parameters are then used to pre-seed the Burp Suite and OWASP ZAP scanner tools, providing more thorough testing of a web application.

"A hacker has all the time in the world to poke and prod at an application, and only needs to find one vulnerability to compromise sensitive data and leave your application at their mercy," said Matt DeLetto, Secure Decisions Security Software Engineer. "So, it's important to thoroughly identify a web application's attack surface. The Attack Surface Detector can help pen testers do just that."

Penetration testers using the ASD plugin have realized substantial time savings by automating the endpoint discovery process. In a recent ASD case study, a CREST-certified penetration

testing company performed an analysis of the same code base with, and without, the use of the ASD plugin and compared the results. Analysts reported an estimated time savings of 4-6 hours in identifying application endpoints and parameters compared to the time it would take to perform the task manually. They also anticipated that code bases of greater size and complexity or of lower quality would have produced even greater time savings.

A command line interface (CLI) version of the Attack Surface Detector provides the ability to detect endpoints without pointing at an active server, or at source code. Endpoints are then imported into Burp and ZAP. In this way the owner of the software IP can provide the valuable ASD information to the independent pen tester without providing the source code for static analysis. This CLI version of ASD was designed to help software owners better protect their software IP, yet still receive the benefits of a thorough pen test from an independent tester.

Another time-saving feature is the *Attack Surface Difference Generator*, which allows pen testers to compare two different versions of the same application and detect endpoints in both versions. Changes in endpoints and parameters between the versions are highlighted, allowing pen testers to focus their testing only on these newly modified areas.

"The value of this tool is clear," said Brianne O'Brien, Secure Decisions Program Manager for ASTAM. "Reduced pen testing efforts through automation and enhanced attack surface pen testing coverage equals time savings and cost savings. Through the ASTAM Program, we strive to build effective application security tools like ASD that can be used to improve the security posture of web applications and reduce an organization's security risk."

Availability

The Attack Surface Detector plugin is open source and freely available for download from the Portswigger BApp Store, the OWASP ZAP Marketplace, and GitHub:

- https://github.com/secdec/attack-surface-detector-zap
- https://github.com/zaproxy/zap-extensions/releases
- https://github.com/secdec/attack-surface-detector-burp
- https://portswigger.net/bappstore

About the ASTAM Program:

The Application Security Technologies and Metrics (ASTAM) program is a U.S. Department of Homeland Security (DHS) Science and Technology Directorate funded project that seeks to improve the security of software through the development and enhancement of technologies that support all aspects of the secure software development lifecycle.

The technologies developed under ASTAM automate techniques used to identify cyber security threats to software applications, improve insight into code testing coverage, make it easier to incorporate AppSec into the software development pipeline, and provide meaningful metrics to security analysts and cyber risk managers about the status, progress, and trends of application security. The program brings automation to the largely manual application security process, developing several technologies as independent capabilities.

About Secure Decisions:

Secure Decisions was created as a division of Applied Visions, Inc. to conduct R&D and develop innovative technologies in cyber security, including application security, security education, network defense, and infrastructure protection. Secure Decisions develops cutting-edge technologies to automate manually-intensive security processes and support the analysis and visualization of large amounts of complex security data. Application security R&D conducted by Secure Decisions led to the development of a new application vulnerability correlation and management system, which is now commercially available through a spin-out company Code Dx, Inc.