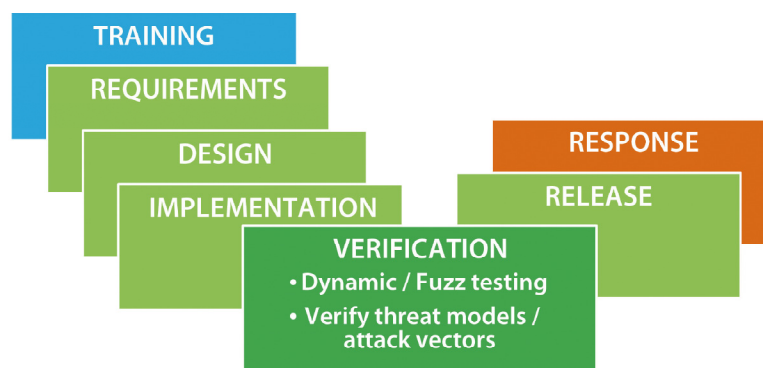




defensics™

FOR MICROSOFT SDL

The increased complexity of new technologies and faster software release cycles are making signature-based security solutions redundant. Instead more adaptable preemptive testing is needed. Moreover, due to outsourcing, the software development process itself is also becoming more complicated creating the need for more powerful project management tools such as software development lifecycle models (SDLC). Microsoft's Security Development Lifecycle (SDL) combines preemptive security testing with the SDLC model. Fuzzing is a natural part of the SDL model, because fuzzing promotes building security into systems proactively, instead protecting vulnerable systems and reacting to security issues.



CODENOMICON Ltd.
info@codenomicon.com
www.codenomicon.com

Tutkijantie 4E
FIN-90590 OULU
FINLAND
+358 424 7431

10670 North Tantau Avenue
Cupertino, CA 95014
UNITED STATES
+1 408 252 4000

25/F., Queen's Road Centre
152 Queen's Road Central
HONG KONG
+852 3426 22900

Fuzzing in the Microsoft's SDL

Microsoft SDL is a world leading software development process model. It is founded on the idea that security should be built into software during the software development process. It basically lists all the security measure that need to be carried out during the development process grouped according to different stages of the SDLC.

For testers the most important phase in the SDL is the verification phase, where fuzzing is used to test the robustness of the system before the release. In the Microsoft SDL fuzzing is used in the verification phase. However, fuzzing can be used throughout the development process from the moment the first software components are ready and even after the release. The earlier the vulnerabilities are found, the easier and cheaper it is to fix them.

What does Codenomicon DEFENSICS™ bring to SDL?

Codenomicon's off-the-shelf DEFENSICS™ solutions provide an easy way to integrate fuzzing into the SDL.

» **NO TEST TOOL CREATION OR MAINTENANCE EFFORT NEEDED:** DEFENSICS™ provides off-the-shelf testing tools for over 150 protocols and file formats. Built-in expertise and automated test case execution facilitate testing.

» **EASY TO INTEGRATE:**

As a software-only platform DEFENSICS™ can be easily integrated into your existing software development and testing processes.

» **FAST TEST RUNS:**

DEFENSICS™ utilizes intelligent model-based test cases. By targeting the test cases the amount of test cases needed has been significantly reduced making the whole testing process quicker and more cost efficient.

The benefits of proactive testing are easy to notice:

» **FIND ZERO-DAY VULNERABILITIES:**

The main strength of Fuzzing is its unparalleled ability to find unknown vulnerabilities. Fuzzing gives testers more time to create and implement patches.

» **SAVE MONEY BY TESTING PROACTIVELY:**

By integrating DEFENSICS™ into your SDL, you can discover flaws at the earliest possible moment. The earlier the bugs are discovered the cheaper and easier it is to fix them.

» **SAVE EVEN MORE BY TESTING EARLIER:**

Codenomicon DEFENSICS™ Traffic Capture Fuzzer enables you to test even earlier. Traffic capture tests are based on real traffic so no specifications are needed.

» **IMPROVE YOUR QoS:**

The costs of bad Quality of Service (QoS) and downtime can be considerable to your company reputation and sales. With Codenomicon DEFENSICS™ you can identify and fix vulnerabilities proactively, before any problems occur.

How does Codenomicon DEFENSICS™ achieve this?

» **REPRESENTS REAL THREATS:**

Fuzzing is essentially doing what the attackers do, but before them. Fuzz tests can also be used to simulate system aging or overload situations.

» **BUILT-IN INTELLIGENCE:**

Codenomicon's intelligent fuzzers are based on protocol specifications, thus they

- **COVER** the entire protocol implementation
- **TARGET** protocol areas most susceptible to vulnerabilities to shorten test run times.
- **IDENTIFY** vulnerabilities in deeper protocol layers.
- **GENUINELY INTEROPERATE** with systems under test (SUT)

» **BUILDS SECURITY INTO YOUR SYSTEM:**

Fuzzing improves the quality of your code ensuring the security of your application. Most security systems merely add to the complexity of your system, making it more vulnerable.

*More information on Fuzzing in Microsoft SDL Pro Network at
<http://www.codenomicon.com/sdl-fuzzing/>*