

## INTRODUCING NEW DEFENSICS X: 10 TIMES THE POWER, 10 TIMES THE EFFICIENCY!

Codonomicon Defensics continues to lead the space in unknown vulnerability management. The latest Defensics 10 (Defensics X) test platform enhances Codonomicon's fuzzing capabilities to provide the highest quality preemptive security testing for network equipment manufacturers, operators, consumer electronics companies, enterprises and governmental organizations.

With Codonomicon Defensics you can proactively discover exploitable zero day (0-day) vulnerabilities. Due to the rise of state sponsored hacking, threats of cyber warfare and unprecedented levels of hacktivism it has become ever more important to manage your threat exposure. Based on the security test technique called fuzzing, Defensics systematically sends invalid and unexpected inputs to the system under test exposing software defects and vulnerabilities more effectively than any other solution on the market.

### DEFENSICS X HIGHLIGHTS:

- Extensive Protocol Coverage
- Improved User Interface
- Scalable Test Cases and Anomaly Control
- Infinite Fuzz Testing
- Adaptive Fuzz Optimizer



### CODENOMICON UNKNOWN VULNERABILITY MANAGEMENT

Since the access into the system or device is enabled by a vulnerability in the code, the number one security priority should be finding and fixing vulnerabilities in both in-house and third-party developed code. Vulnerability management is often understood as scanning for known vulnerabilities, but finding the unknown vulnerabilities is equally important.

# FEATURE HIGHLIGHTS



## EXTENSIVE PROTOCOL COVERAGE

Defensics generational (model based) fuzz testing modules are available in over 200 standard network protocols. These tests can be further enhanced with Defensics Universal and Traffic Capture fuzzing modules, with which you can now fuzz any network protocol, service interface or application file format.

## FULLY MODEL-BASED FUZZERS

Defensics test suites are based on deep protocol models. Test cases are created automatically, no need for manual test case creation! Model-based fuzzers emulate a protocol or file format interface, allowing them to understand the inner workings of the tested interface. For this reason, tests are able to penetrate much deeper within the system under test, reaching all the way into the state machine and even output generation routines.

## INTUITIVE AND EXTENSIBLE

Easy to use test solution gets you up-to-speed quickly. Clear and logical user interface will guide you through every step of the testing process. A command-line interface that supports third party tools and scripts is also available.

## FAST, AUTOMATED TEST RUNS

The faster you can execute tests, the more tests you can run and more vulnerabilities you will find. Defensics can generate and run thousands of test cases per second!

## ACCURATE, ACTIONABLE REPORTS

Defensics provides accurate reports that are easy to interpret and act upon. The reports have direct links to test cases identifying specific problems, which helps sharing detailed test results within your organization. Identified flaws are absolutely repeatable and traceable. The immediate failure reproduction facilitates prompt reaction and fix verification.

## DEFENSICS FEATURES

- Broadest protocol coverage
- Proven test methodology and technology
- Scalable, prebuilt test cases
- Test case editing
- Fast, automated test runs
- Complete and comprehensive documentation
- Accurate, actionable reports
- Immediate reproduction and regression
- Automatic updates
- Software flexibility
- Intuitive and extensible
- Clear and logical user interface
- XML Anomalization Engine
- PCAP I/O
- Traffic Capture Fuzzing
- Quality and security test best practices

For a detailed description of Defensics features, visit <http://www.codenomicon.com/defensics/>