



 CODENOMICON

PROACTIVE **CYBER DEFENSE**

STAY AHEAD OF THE ATTACK

PROACTIVE SECURITY SOLUTIONS FOR NETWORKS
AND CRITICAL INFRASTRUCTURE

The Codenomicon Advantage

Codenomicon Defensics™

Defensics is a product family of automated proactive software testing solutions for all protocols. It achieves unparalleled efficiency in finding both known and unknown vulnerabilities.

- > TEST AGAINST REAL CYBERSECURITY THREATS
- > HARDEN SYSTEMS BEFORE DEPLOYMENT
- > MITIGATE CYBER SECURITY RISKS
- > IMPROVE QUALITY OF SERVICE

CUSTOMERS: Governmental organizations and Private companies, for example Cisco Systems, AT&T, Microsoft.

Network Analyzer

The Network Analyzer is a software-based tool for traffic audit, documentation and analysis. Use the Network Analyzer to see what is really happening in your network.

- > DECREASE DOWNTIME
- > GAIN SITUATIONAL AWARENESS
- > CLARIFY COMPLEX SYSTEMS
- > OPTIMIZE NETWORK TESTING AND SECURITY

CUSTOMERS: Governmental institutions, critical infrastructure providers, research organizations.

Professional Services

With our professional services, you can enjoy the full benefit of our testing tool and security expertise.

- > **TURN-KEY SOLUTIONS:** We will do everything from mapping your monitoring system to planning the deployment and installing and configuring the system for you.

The Internet has become a critical resource for the civilian, defense and intelligence operations of governments. However, critical networks like telecommunication networks, power grids, energy pipelines, refineries and financial networks are essential for the functioning of a society, but they were designed to be isolated systems, not a part of a global network.

Test

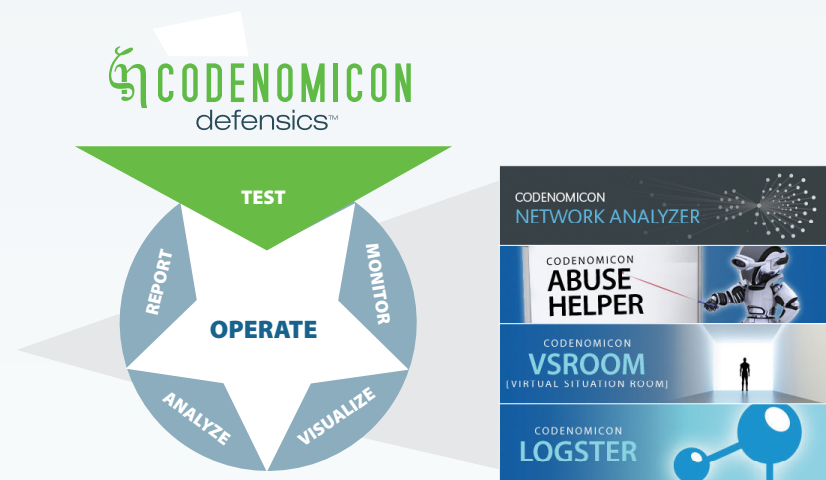
> **Codenomicon Defensics:** Find and fix known and previously unknown vulnerabilities, before anyone has a chance to exploit them. In all types of cyber attacks, the initial access is enabled by a software vulnerability.

Monitor

> **Codenomicon Network Analyzer:** Monitor network traffic and see what is really happening in your network.

> **Codenomicon Abuse Helper:** Automatically collect and process existing abuse information.

> **Codenomicon Vsroom:** Collect information from different monitoring systems into one browser based user interface.



Visualize

> **Codenomicon Network Analyzer and VSRoom:** Automatically create interactive visualizations, which allow you to drill up and down from high-level views to individual packet data.

Analyze

> **Codenomicon Network Analyzer and VSRoom:** The high-level visualizations summarize the status of critical networks and assets helping you to make better informed decisions faster. Use the drill-down options to investigate incidents further.

Report

> **Codenomicon Network Analyzer, Abuse Helper and VSRoom:** Use automated, actionable reporting features and collaboration tools to share information with your partners and stakeholders.

The Codenomicon Benefits

Gets rid of vulnerabilities, before they are exploited

GOVERNMENT PROCUREMENT OFFICER OR CRITICAL SERVICE PROVIDER

- **USE ROBUSTNESS AS A SELECTION CRITERIA:** Use Defensics to test the robustness of competing products, before making your decision.
- **AVOID DEPLOYMENT DELAYS AND FUTURE INCIDENTS:** Test third party software before integration and encourage contractors to use Defensics during development.

Reveals what is really happening in your networks

CRITICAL SERVICE PROVIDER, CRITICAL INFRASTRUCTURE PROTECTION PROFESSIONAL OR 24/7 SITUATION OFFICER

- **CLARIFY COMPLEX SYSTEMS:** Discover undocumented software behavior, access violations, infected hosts, obsolete protocols etc. Get rid of redundant elements.
- **OPTIMIZE NETWORK TESTING AND SECURITY:** See what is really happening in your network and base your actions on facts rather than assumptions.

Automates abuse information collection, processing and reporting

CERT SECURITY OFFICER OR CYBER SECURITY TEAM MEMBER

- **PROCESS MORE ABUSE INFORMATION:** The Abuse Helper automatically collects relevant real-time abuse information and compares real-time abuse information to earlier records to find out more, and sends out actionable reports.

CRITICAL SERVICE PROVIDER

- **RECEIVE RELEVANT ABUSE INFORMATION:** The reports contain real-time abuse information about incident requiring action.

Displays the status of critical assets in one view

DECISION-MAKER, CRITICAL INFRASTRUCTURE PROTECTION PROFESSIONAL OR 24/7 SITUATION OFFICER

- **MAKE BETTER INFORMED DECISIONS FASTER:** Use situational awareness and incident records to prioritize the allocation of resources, make budget plans based on incident history and to decide whether to raise alertness.

Informs stakeholders

CERT SECURITY OFFICER OR CYBER SECURITY TEAM MEMBER, DECISION-MAKER, CRITICAL INFRASTRUCTURE PROTECTION PROFESSIONAL OR 24/7 SITUATION OFFICER

- **SEND AUTOMATED, ACTIONABLE REPORTS:** Send automated reports containing relevant abuse information.
- **SHARE SITUATIONAL AWARENESS:** Browser-based views and collaboration tools enable you to share real-time situational awareness information.

Helps reveal the criminal infrastructure behind attacks

CYBERCRIME INVESTIGATOR:

- **LOOK FOR IDENTITIES, NOT FINGERPRINTS:** The AbuseHelper automatically searches for related events delivering more information on identities connected to incidents, such as related IP addresses, the type malware they associated with and their geographic location.

Abuse Helper

The Abuse Helper is a centralized system for collecting, processing and reporting openly available abuse and incident information on your networks.

- > EARLY WARNING SYSTEM
- > AUTOMATED, ACTIONABLE REPORTS

VSRoom

The VSRoom is a real-time visual monitoring solution for systems monitoring cyber incidents and critical infrastructure and assets.

- > OBSERVE THE STATUS OF CRITICAL ASSETS IN ONE GLANCE
- > BROWSER-BASED VIEWS AND COLLABORATION

USERS: Estonian Government

Common Features

- > BOTNET INSPIRED ARCHITECTURE
- > AUTOMATED ABUSE INFORMATION HANDLING
- > DISCOVER INCIDENTS PROACTIVELY

Logster

The Logster provides a video summary of network events. It replays millions of web log entries recorded over extensive periods of time displaying them in earth view.

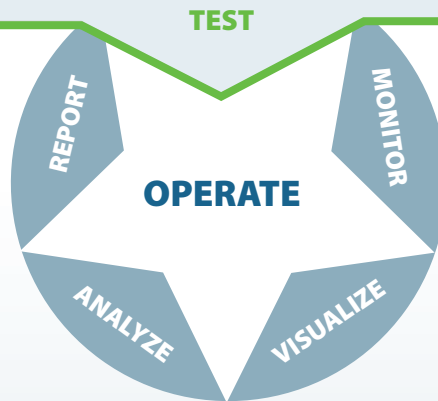


www.codenomicon.com

Codenomicon Solutions for Unknown Vulnerability Management (UVM)



BEFORE DEPLOYMENT: FIND AND FIX KNOWN AND UNKNOWN VULNERABILITIES.



DEPLOYED SYSTEMS: IDENTIFY, REPORT AND ADDRESS INCIDENTS AND INFECTIONS FASTER AND MORE EFFICIENTLY.



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

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

12930 Saratoga Avenue, Suite B-1
Saratoga, CA 95070
UNITED STATES
+1 408 252 4000

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

21 Science Park Road
#02-01 The Aquarius
SINGAPORE 117628
+65 9186 8174