

An iceberg floating in the ocean. The tip of the iceberg is above the water line, representing known vulnerabilities. The much larger part of the iceberg is submerged below the water line, representing unknown vulnerabilities. The sky is blue with light clouds, and the water is a deep blue.

**KNOWN**  
VULNERABILITIES

What you can find with your *current* security tests.

**UNKNOWN**  
VULNERABILITIES

What *Codenomicon* can help you reveal.

Codenomicon whitepaper:

# Unknown Vulnerability Management

- Anna-Maija Juuso and Ari Takanen -



CODENOMICON Ltd. | [info@codenomicon.com](mailto:info@codenomicon.com) | [www.codenomicon.com](http://www.codenomicon.com)

Tutkijantie 4E | FIN-90570 OULU | FINLAND | +358 424 7431  
10670 North Tantau Avenue | Cupertino, CA 95014 | UNITED STATES | +1 408 252 4000

---

PREEMPTIVE SECURITY AND ROBUSTNESS TESTING SOLUTIONS

# 1 Introduction

The greatest security challenge for enterprises today is discovering unknown vulnerabilities hiding in software. Software release cycles are getting faster and new technologies are increasingly complex, creating a perfect breeding ground for security-related bugs. New patches are released every week, each requiring immediate attention. The maintenance downtime alone is expensive. Not to mention the costs of ad-hoc deployment, which is also prone to errors. At the same time, a growing share of vulnerabilities is never disclosed publicly. Instead, they are sold and distributed within underground hacker communities. Companies can no longer afford to wait for patch releases from vendors, nor can they rely on user communities to find and report these bugs. Thus, there is a need for new proactive ways to protect products and services.

*It's what you don't know  
that makes you vulnerable*

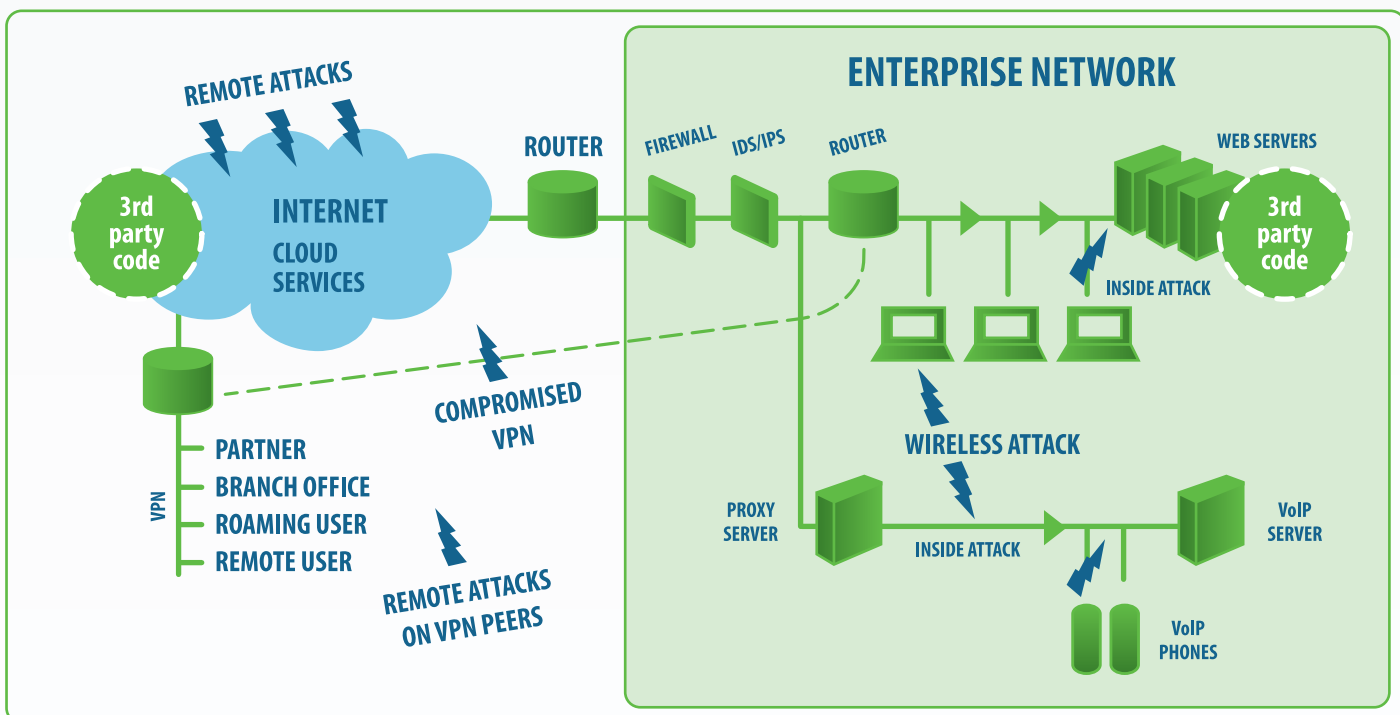


Figure 1: Threats within an Enterprise Network

## 2 Biggest Threat to IT Security: Unknown Vulnerabilities

Unknown vulnerabilities are exploitable bugs hidden in software code. In contrast to known disclosed vulnerabilities with available patches and updates, vendors are unaware of the existence of these unknown bugs, and therefore they are not prepared to provide fixes for them. Vulnerabilities in customer-facing applications provide the easiest and most frequently used way for hackers to attack an enterprise. Thus, finding and fixing vulnerabilities in your own and outsourced code development should be a top priority. It is useless trying to protect an impaired system or application with firewalls and antivirus software. These merely add to the complexity of the system, and complexity is always a threat, because it increases the attack surface of the system. For example, if hackers manage to compromise another user in your VPN network, they gain direct entry into your network. Indeed, the more complex your system or network, the more hidden attack surfaces there are. By recording actual traffic in your network and examining it, you can reveal vulnerable interfaces that you were not aware of and even discover possible zero-day exploits in action.

## 3 Discover Security Issues Proactively, Don't React to Them

Unknown vulnerabilities can cause a lot of havoc for companies. Attacks against unknown vulnerability can go undetected and once the attack is discovered, the repair process tends to be slow, because there are no ready patches or updates available. All the while, customers are unable to access your service, or even worse: their safety is endangered. Installing new patches also causes downtime. All the downtime and problems are bad to your company reputation and ultimately your sales. Wouldn't it be much better to discover security issues proactively and then deploy all the fixes at the same time? By finding and fixing vulnerabilities proactively, you also have time to verify the fixes.

## 4 Codenomicon Defensics for Unknown Vulnerability Management

Unknown Vulnerability Management is the process of proactively identifying and mitigating threats caused by unknown vulnerabilities. It is applicable both before and after deployment and can be used to ensure the security and robustness of both in-house and third party software productions. The Codenomicon Defensics model for Unknown Vulnerability Management consists of four phases: Analysis, Testing, Reporting and Mitigation. Unlike legacy vulnerability management processes, fuzzing does not require a vulnerability assessment phase, because, in fuzzing, there are no false positives and therefore all the found vulnerabilities are critical

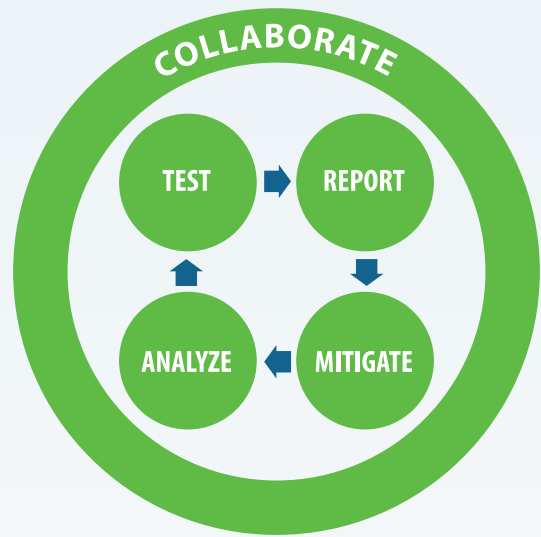


Figure 2: Unknown Vulnerability Management

### Analyze

Use the Codenomicon Network Analyzer to map real network traffic and to determine what needs to be tested within your network. The Analyzer records traffic at multiple points in your network, thus it can capture the entire traffic in your network. It then automatically creates visualizations illustrating different aspects of the captured data. You can drill up and down from looking at high-level visualizations to inspecting the corresponding packet data, even in real time, and reveal hidden interfaces and possible exploits.

### Test

Run multiple test suites simultaneously and discover both known and previously unknown vulnerabilities with unparalleled efficiency. Codenomicon's Defensics product family contains intelligent specification based tools for over 200 protocols and file formats. Specification based tools contain all the possible protocol messages, and thus they can genuinely interoperate with the tested system exposing vulnerabilities even in deeper protocol layers. Unlike most XML Fuzzers, the state-aware Defensics XML Fuzzer not only tests XML parsers, but also all XML applications. The Traffic Capture Fuzzer creates tests from real traffic and can be used to test all protocols, and Generic File Format Fuzzer tests all file formats.

### Report

Codemicon test suites generate different types of reports for different audiences. Management reports provide a high-level overview of the test execution. Log files and spreadsheets help you to identify troublesome tests and to minimize false negatives. You can facilitate the technical analysis of individual tests by augmenting the already extensive test case documentation with PCAP traffic recordings. In addition, all important information is automatically collected into a Remediation Package, which you can send to third parties for automated reproduction.

### **Mitigate**

Use the automatic features Defensics provides to quickly and easily reproduce vulnerabilities, perform regression testing and verify patches. The Codenomicon Defensics test suites automatically generate reports, which contain CWE values for the found vulnerabilities and direct links to the test suites that triggered the vulnerabilities. The CWE values help testers decide which vulnerabilities should be fixed first. Defensics also makes it easier to identify the test cases that triggered the vulnerability, to reproduce vulnerabilities and to verify patches. The test case documentation can be used to create tailored IDS rules to block possible zero-day attacks.

### **Collaborate**

Manage tests carried out in multiple locations, process test results and coordinate the repair process in the Codenomicon Collaboration environment. In companies and organizations, the testing resources are often spread across geographical locations. The Collaboration enables users to remotely access the same system, thus they can execute the same tests, share results and other documentation, and reproduce the same vulnerabilities.

### **Services**

Codonomicon also provides a number of security services ranging from creating custom tools to trial tests and coordinating the process of fixing the found vulnerabilities.

## **5** Benefits of Unknown Vulnerability Management

Codonomicon's Defensics test tools help you to secure your networks and applications from known and previously unknown protocol-level attacks. With the Codenomicon Network Analyzer, you can find those hidden interfaces, and with the Codenomicon Defensics test tools, you can find and mitigate vulnerabilities in applications and systems, before the hackers have a chance to exploit them.

### **Save Resources**

The earlier vulnerabilities are found the easier and cheaper it is to fix them and the more thorough the fixes are. Moreover, if vulnerabilities are fixed, before the software is released, then there will not be any vulnerabilities for hackers to exploit.

### **No more Patch Rat Race**

By finding and mitigating security issues proactively, you can avoid getting stuck in the endless rat race of deploying yet another patch, before attackers can create an exploit. By managing unknown vulnerabilities, you can anticipate upcoming patch releases and patch deployment no longer has to be a constant crisis management process. You can notify your customers of upcoming patch releases beforehand and deploy all patches in one well planned security initiative. After all, downtime is always costly.

### **Extending Vulnerability Feeds**

With the Defensics Traffic Capture Fuzzer you can generate tests from different types of third party vulnerability feeds and use these to test systems for similar weaknesses. As soon as the relevant security advisories and vulnerability information are released, you can test whether the same vulnerabilities apply to your system. Sometimes, the vulnerability feed providers deliver the actual exploits as PCAP traffic recordings that you can use these directly to generate tests. However, in many cases, the vulnerability feed just contains general information on how to reproduce the vulnerability. In these cases, you can use Codenomicon Network Analyzer to generate an exploit PCAP for generating tests.

### **Build Defenses against Zero Day Attacks**

Help your firewall block attacks unknown vulnerabilities by using the extensive documentation that Defensics provides. The test cases triggering vulnerabilities in your system are described clearly making it easy to write your own IDS (intrusion detection system) rules. The rules can be based on vulnerabilities found by running predefined Defensics tests, or testing around known vulnerabilities downloaded from third party vulnerability feeds. You can also use Defensics to generate variations of the original attack and to test how well IDS/IPS systems and firewalls can detect and block both the original attack and variations of it.

### **Better Patches**

By investigating security issues proactively, you gain more time and you can create better patches and also have time to test them. However, vendors usually create patches under considerable time pressure, and sometimes the quality of patches is not as good as it should be. By using Codenomicon's Defensics fuzzers you can easily verify the quality of patches by testing them with variations of the original attack. Sometimes, even slight variations of the original attack can trigger new vulnerabilities.

## **6** The Real Benefits

The deployment of new technologies always involves a risk of unpredictable security, quality and interoperability issues. The source of this unpredictability is unknown vulnerabilities in the software. Codenomicon's Unknown Vulnerability Management Tools help you find and fix unknown vulnerabilities enabling you to gain more control over the development and deployment process and to avoid any undesirable security, quality and interoperability shortcomings that might affect the customer experience.