

CSaaS

Codonomicon Security as a Service

Codonomicon's Security as a Service (CSaaS) solution enables Web2.0 style integration for all proactive security measures - for the very first time. Now IT Ecosystems, Service Providers, Vendors, Vendors' vendors, contractors and consultants can all work together in a truly collaborative environment - sharing scenarios, environments, test target configurations, test cases, results with each other where ever they are in the world. With this solution, you will enable cost-savings through more effective integration of multi-team and multi-contractor services.

Figure 1.

The **problem** with outsourced testing

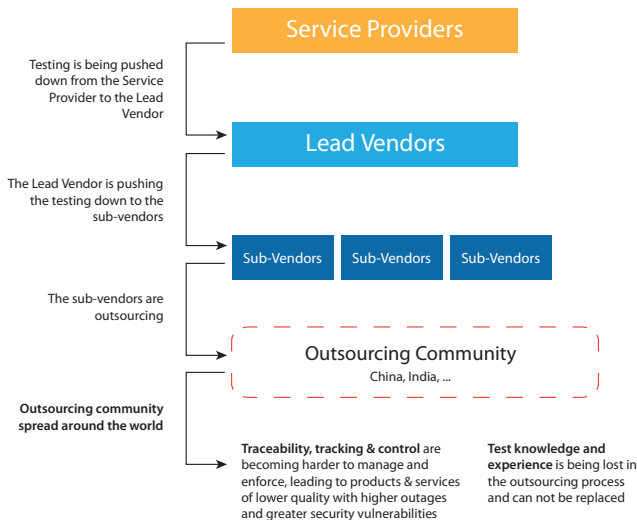


Figure 2.

How to **overcome** these issues?

Codonomicon Security as a Service:
Service layers

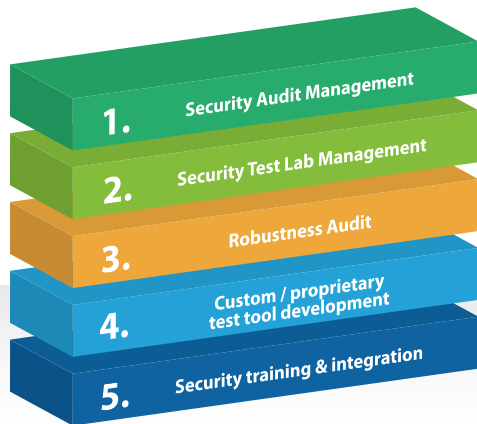


CODENOMICON Ltd.
info@codenomicon.com
www.codenomicon.com

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

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

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



Security Audit Management

Some Jurisdictions require that companies and organizations have their security systems audited by an independent 3rd party a few times a year. It is often very hard for the organization being audited to make sense of these reports, especially when they come in different formats from different audit vendors - with different audit techniques and focuses.

Codenomicon's offering allows the company being audited to organize and manage this data in such a way that the audit results can be imported, organized, searched and better understood to normalize against the variables incorporated by the audit vendors.

Security Test Lab Collaboration and Management

As shown in the Figure 1, it can be seen that test resources are now much more widely spread across labs, countries and even disciplines. Service Providers are mandating a scheme whereby audit of results and result sharing is possible. NEMs, active in the lead vendor role are looking for a way to roll up collated test results from their sub-vendors and the outsourcing community. Less about automation and more about collaboration and results sharing.

Codenomicon's offering allows Service Providers to better understand what their vendor community is testing, how, with which test methodologies, where and by whom. Where Service Providers have their own in-house testing capabilities it allows them to coordinate efforts and collaboratively work on creating test plans and sharing results / environments.

The offering allows lead vendors to manage their vendor and outsourcing communities, and to provide auditing capability of abstracted results up to their customers. Web 2.0 meets the test and security industry for the first time.

Robustness Audit

As shown in the Figure 1, it can be seen that there is less test resources to carry out testing. There is also often less experience within a department able to run robustness testing. Secondly as testing is outsourced there is less facility for sub-vendors and outsourcing companies to purchase commercial testing tools.

Codenomicon's offering allows for companies to outsource their Robustness testing to expert resources on a pay-for-service engagement basis, overcoming any lack of in-house resources. This service offering also allows smaller companies and specifically outsourcers to get access to tools they may ordinarily not be able to afford.

Custom / Proprietary Test Tool Development

Many company's employ non-published standards which are generally employed in internal facing interfaces between devices from the same vendor or where there's no need for the interface to face an external device not from the same company. Also with a great many standards these days, proprietary extensions are readily written which extend the functionality of openly described public standards.

Codenomicon's offering allows for companies to have Robustness or Vulnerability test tools written for their extensions or internal protocol interface points. The service is based on working closely with the company needing the protocol tested and will allow the company to better understand if there are any security issues in either proprietary extensions or on non-public interface points.

Security Training and Security Test Methodology Integration

With reference to the 'outsourced testing' diagram, it can be seen that departments are relying more and more on outsourcing experts to not only perform the testing function, but to decide on which test methodologies are the correct ones to carry out during the testing phase. Very often the wrong type of testing is performed, but more importantly the correct type of testing is not being performed at the correct times in accordance with both product and security life cycle guidelines and best-practices.

Codenomicon's offering allows companies to take back testing and instruct lead vendors, sub-vendors and the outsourcing community by advising of the correct requirements, guidelines and best practices for the type of testing along the product and security life cycle.

Codenomicon also advises on how to integrate it's Negative / Robustness / Fuzzing test methodology in to existing test campaigns, advising on when in the life cycle to this type of testing and how to achieve the best results when integrated with existing test automation, control & management harnesses.