AWARD-WINNING CYBERSECURITY

The increasingly networked nature of governments, banks and many other critical infrastructures make them increasingly vulnerable to cyberattack. ADAX's relentless focus on market needs resulted in a range of innovative cyberdefence products and services.

"The key to handling cyberattacks is to detect, analyse and react quickly," emphasises Adrien Bécue of Airbus DS Cybersecurity. "But this is a fast-moving field: the systems you put in place last year may not even detect the attacks you'll get tomorrow. Cyberdefences need to constantly evolve."

Constant evolution was therefore the defining characteristic of the EUREKA ITEA -2 Cluster project Attack Detection And Countermeasures Simulation (ADAX), which won the 2017 EUREKA innovation award. Involving 8 companies and research institutes from France and Turkey, it began in early 2013 with a focus on defending organisations against Distributed Denial of Service (DDoS) attacks.

At that time, the banking sector was still reeling from a large DDoS on global payment systems by the "Anonymous" hacktivist group. By mid-project, however, the focus had changed to an emerging class of Advanced Persistent Threats (APTs). "We discovered an APT called "Pitty Tiger" on the IT network of one of our customers," Bécue recalls. "It got there via a phishing e-mail containing a corrupted Word document, which placed software on their server capable of sending confidential information to the hackers."

Pivot to meet the threat

With threats getting more and more sophisticated, the consortium pivoted. Bécue credits this emphasis on end-user needs to the inclusion of Yapi Kredi Bank as end user and pilot owner within the consortium. This helped resist "the dreadful temptation to do engineering for engineers. We started out focused on shortening reaction times, but our banking partners' direct involvement in the project made us realise that we needed to help optimise their response, not just shorten it."

The partners therefore developed and integrated advanced decision support tools, enabled by attack and countermeasure simulation capabilities, to optimise 'Return-On-Response-Investment' (RORI), a new metric for cost/benefit analyses of

> ❝ *We resisted the temptation to do engineering for engineers and pivoted to meet user needs value*

the many countermeasures that could be implemented in response to any attack.

By proposing optimised response plans, backed up by quantified metrics, they showed business owners could cut resolution times from 3 hours to 90 minutes based on a defined attack scenario.

New products, clients and patents

An array of technological and commercial results followed. The academic partners produced no less than 30 articles, 7 theses, 2 patents and 2 conference events, for example, with Institut Mines-Télécom (France) patenting their RORI assessment mechanism.

By early 2017, the commercial partners have already launched new products and registered at least 12 new customer contracts. In France, for example, Airbus DS Cybersecurity added dedicated modules to their Cymerius® security supervision software and registered new sales in the financial, military, retail, space and oil/gas sectors, while SME 6Cure delivered its remote countermeasure enforcement tool to protect a European champion in telecom services.

The picture is similar for the Turkish SMEs in the project: PlusOneMinusOne won major new contracts with telecom and transaction companies for their hybrid attack detection system, while Provus sold its dynamic knowledge and model acquisition tool to Mastercard. Yapi Kredi Bank, finally, implemented the full ADAX system on its IT network in Turkey, supporting 5000 users.

MAIN PARTNER

Cassidian Cybersecurity (Airbus DS Cybersecurity), France
https://www.cybersecurity-airbusds.com/
adrien.becue@airbus.com

OTHER PARTNERS

Yapi ve Kredi Bankası
Netasq
PlusOneMinusOne
6Cure
Bogazici University
Institut Mines-Télécom

TOTAL R&D INVESTMENT

€ 6.6 M

DURATION

January 2013 to April 2015

COUNTRIES INVOLVED

EUREKA is a European network for market-oriented R&D.