ADAX

Business excellence in cybersecurity

Impact highlights

- For a random set of attack scenarios, a decision time-saving from 1 hour to 3 minutes and a reduction in average response cost from €271 k to €100 k was achieved.
- A total of 12 customer contracts have been reported directly linked with the project results, addressing diverse vertical markets like finance, military, retail, space and oil & gas.
- ADAX is known to have directly contributed to €7 m of the €33 m turnover recorded by Cassidian Cybersecurity SAS in 2014 and led to the recruitment of 6 engineers. By 2016, all developments from ADAX had been embedded in the Cymerius® commercial version.
- The mixed-signature based intrusion prevention system developed by NETASQ has been deployed by Stormshield on more than 10,000 appliances.
- Yapi Kredi Bank has demonstrated the full ADAX system on its IT network in Gebze (Turkey), supporting 5,000 users.
- The SMEs in the project consortium, like 6cure, P1M1 and Provus, have delivered key innovations which are being largely adopted by the market. For example, the MAMAT tool developed by Provus is used by MasterCard to model its ATM management systems (PAYS).

Cybersecurity is vital to any person or entity, from consumer to government, involved in conveying information. The key lies in being able to detect attacks and react quickly and efficiently by launching appropriate countermeasures. While a number of commercial off-the-shelf cyberdefence tools exist, there is a clear need in today's market for detection to be extended with reaction capabilities and support mechanisms to enable security operators to make informed decisions in a dynamic situation. The ITEA 2 project ADAX has delivered a set of key innovations improving prevention, detection, decision support, countermeasure enforcement and knowledge management to support security operation on complex and critical IT infrastructures.

Project results

Innovations include a hybrid detection technique in which behaviour-based and signature-based detection are combined. The former is a probabilistic approach that helps to identify new attacks (0-day attacks) while the latter is a deterministic approach that is largely applied to known attacks. Combining both techniques helps improve detection rates, lower false-alarm rates and shortens the detection time, saving both time and costs for customers and security service providers in the detection phase.

Improved detection of new complex attacks (detection rate of 98.7% and false alarm rate <1%) and acceleration of the detection-to-remediation loop resulted from the development of enhanced decision-support tools along with a network simulation tool to enable attack and countermeasure impact to be assessed before implementation on a real IT infrastructure. A new metric, 'Return-On-Response-Investment' (RORI), was set up to calculate the 'cost-benefit' of the different countermeasures that can be implemented to remediate to a particular attack.

A complete ADAX advanced simulation environment, consisting of different interacting modules supplied by different partners, was delivered and demonstrated in a real environment at the premises of Turkish project partner and on-board end user Yapi Kredi Bank.

Exploitation

Airbus DS Cybersecurity added the countermeasure optimisation tool to Cymerius® security supervision software for exploitation by its Security Operation Centre and it is also available as a software product, with 5 key contracts awarded by key customers from the financial, defence, retail, oil&gas and space sectors. The added value of ADAX quantified cyber-risk assessment capability has been recognised by the Federation of European Risk Managers (FERMA) and will be integrated in Airbus Cybersecurity portfolio under the brand of "CyPRES-RM®".

Institut Mines-Télécom developed and patented a mechanism to assess the impact of attacks and countermeasures on multiple criteria (Attack Volume Mechanism) and to quantify the RORI to improve the quality and cost of the remediation.

The Intrusion prevention mechanism developed by NETASQ is embedded in the new Stormshield Network security appliance, providing mixed-signature detection capability with lower false alarm rate.

6cure developed the Countermeasure enforcement tool, providing automated construction, deployment, accounting and deployment of countermeasures to shorten remediation time. This made it possible to deploy countermeasures in seconds, instead of the minutes or hours it previously took for manual operations. This resulted in the company being awarded a contract with a French Internet Service Provider.

P1M1 developed the Intrusion detection system, providing hybrid detection capability with improved detection rate regarding new attacks, for which it was awarded contracts with 2 major telecom & transaction companies and a major financial institution.

Provus developed the Model acquisition and maintenance (MAMAT), providing automated large scale information network modelling capability, saving time for experts in network topology activities. MasterCard now uses the MAMAT tool to model ATM management systems (PAYS) to analyse and strengthen security.

10030

ADAX

PROJECT LEADER
Adrien Philippe Bécue,
Cassidian Cybersecurity

PROJECT START
January 2013

PROJECT END
April 2015

PROJECT WEBSITE
http://adax.boun.edu.tr

PARTNERS

France

6cure	⊙
Cassidian Cybersecurity	●
Institut Mines-Télécom	◉
NETASQ	⊙

Turkey

Bogazici University	◉
PlusOneMinusOne	⊙
Provus A.S.	⊙
Yapi Kredi Bank	●