ITEA Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands

T + 31 88 003 6136
E info@itea3.org
W www.itea3.org

ITEA 3 is a EUREKA strategic ICT cluster programme

Exploitable Results by Third Parties

10030 ADAX

Project details

Project leader:	Adrien Bécue
Email:	Adrien.becue@airbus.com
Website:	http://adax.boun.edu.tr/

Name: Intrusion Prevention System		
Input(s):	Main feature(s):	Output(s):
▪ Internet traffic	▪ Mixed signature detection	▪ Automatic reactions ▪ Alerts

Unique Selling Proposition(s):	▪ Finer, faster detection, less false positives, better performance (as partial signatures are simpler)
Integration constraint(s):	▪ Cannot combine signatures on two distinct connections ▪ Tailored to Stormshield Endpoint UTM appliance
Intended user(s):	▪ Stormshield Endpoint customers: enterprise UTM market
Provider:	▪ NETASQ
Contact point:	▪ Fabien Thomas (fabien.thomas@netasq.com)
Condition(s) for reuse:	▪ Commercial license to be negotiated

Latest update: 03/06/15

Name: Intrusion Detection System		
Input(s):	Main feature(s)	Output(s):
▪ Traffic	▪ Hybrid attack detection	▪ Alerts ▪ Warnings

Unique Selling Proposition(s):	▪ Gathers advantages of signature-based detection (deterministic detection of known attacks) and behavior-based detection (probabilistic detection of unknown attacks).
Integration constraint(s):	▪ Requires tailored definition of normal versus abnormal traffic ▪ Requires (human) post-analysis of anomaly warnings
Intended user(s):	▪ Mainly required by banking and e-commerce to deal with DDoS attacks.
Provider:	▪ P1M1
Contact point:	▪ Tolga Kurt (tolga.kurt@p1m1.com)
Condition(s) for reuse:	▪ Commercial license to be negotiated

Latest update: 03/06/15

Name: Decision Support & Reaction Tool		
Input(s):	Main feature(s)	Output(s):
▪ Annual Loss Expectancy (ALE) ▪ Annual Infrastructure Value (AIV) ▪ Risk Mitigation (RM) ▪ Annual Response Cost (ARC)	▪ Attack Volume Application ▪ RORI Application (Return On Response Investment)	▪ Graphical 3D representation of attacks and countermeasures ▪ List of selected countermeasures

Unique Selling Proposition(s):	▪ Graphical user-interface enabling faster decision making ▪ RORI metric enables optimal countermeasure selection, particularly required by safety-driven and business-driven environments
Integration constraint(s):	▪ To date : tailored to Stormshield Endpoint UTM ▪ Support of other types of firewalls planned
Intended user(s):	▪ Managed Security Services Providers (MSSP) ▪ Banks & financial sector ▪ Critical Infrastructures
Provider:	▪ Institute Mines Telecom
Contact point:	▪ Gustavo GONZALEZ (gustavo.gonzalez_granadillo@telecom-sudparis.eu)
Condition(s) for reuse:	▪ Patent acquisition

Latest update: 03/06/15

Name: Decision Engine		
Input(s):	Main feature(s)	Output(s):
▪ Incident ▪ Security context ▪ Asset model	▪ Decision support ▪ Automatic UTM reconfiguration	▪ Response plan ▪ UTM/Firewall reconfiguration orders

Unique Selling Proposition(s):	▪ Automated enforcement of countermeasures ▪ Remote & automated reconfiguration of UTM
Integration constraint(s):	▪ Tailored to Stormshield Endpoint UTM ▪ Tailored to 6CURE Countermeasure Enforcement module
Intended user(s):	▪ Mainly required by banking and e-commerce to deal with DDoS attacks.
Provider:	▪ Cassidian Cybersecurity SAS
Contact point:	▪ Christophe Ponchel (Christophe.ponchel@airbus.com)
Condition(s) for reuse:	▪ Commercial license to be negotiated
	Latest update: 03/06/15

Name: Countermeasure Enforcement		
Input(s):	Main feature(s)	Output(s):
▪ Network-level identification of communications to prohibit (source, destination, protocol and/or service)	▪ Automatisation of firewall reconfiguration for countermeasure application ▪ Accounting and tracking (by who, when, active or not) countermeasures	▪ Firewall reconfiguration orders

Unique Selling Proposition(s):	▪ Automation of construction, deployment, and accounting of countermeasures ▪ Tailored to DDoS attack countermeasure enforcement ▪ Fast and tailored temporary firewall rules enforcement ▪ Integration with a solution (6cure TM) covering management of other types of countermeasures as well ▪ Make better use of existing infrastructure (firewalls)
Integration constraint(s):	▪ Full version with GUI integrates with 6cure TM ▪ Stand-alone version without GUI integrates with Cassidian Decision Engine ▪ Current firewall management is compatible with netfilter firewalls (extensible)
Intended user(s):	▪ Medium to large enterprises, operators, hosting providers, government
Provider:	▪ 6cure
Contact point:	▪ Jouni Viinikka (jvi@6cure.com)
Condition(s) for reuse:	▪ Commercial license to be negotiated

Latest update: 03/06/15

Name: Model Acquisition and Maintenance Tool		
Input(s):	Main feature(s)	Output(s):
▪ CMDB ▪ Network scans ▪ SNMP messages	▪ User-driven data feeding ▪ Inventory ▪ Agent based data feeding ▪ Knowledge base	▪ AADL system representation ▪ Hardware & software inventory

Unique Selling Proposition(s):	▪ Provides automated large scale information networks models ▪ Provides knowledge base support to detection, decision and countermeasure enforcement capabilities components
Integration constraint(s):	▪ Requires inputs from a configuration management database (CMDB) ▪ Requires tailored interfaces to supported detection, decision & countermeasure enforcement components.
Intended user(s):	▪ MSSPs, Enterprises, Critical Infrastructures, Banking & financial services
Provider:	▪ PROVUS
Contact point:	▪ Gürkan Gür (gurkan.gur@provus.com.tr)
Condition(s) for reuse:	▪ Commercial license to be negotiated
	Latest update: 03/06/15