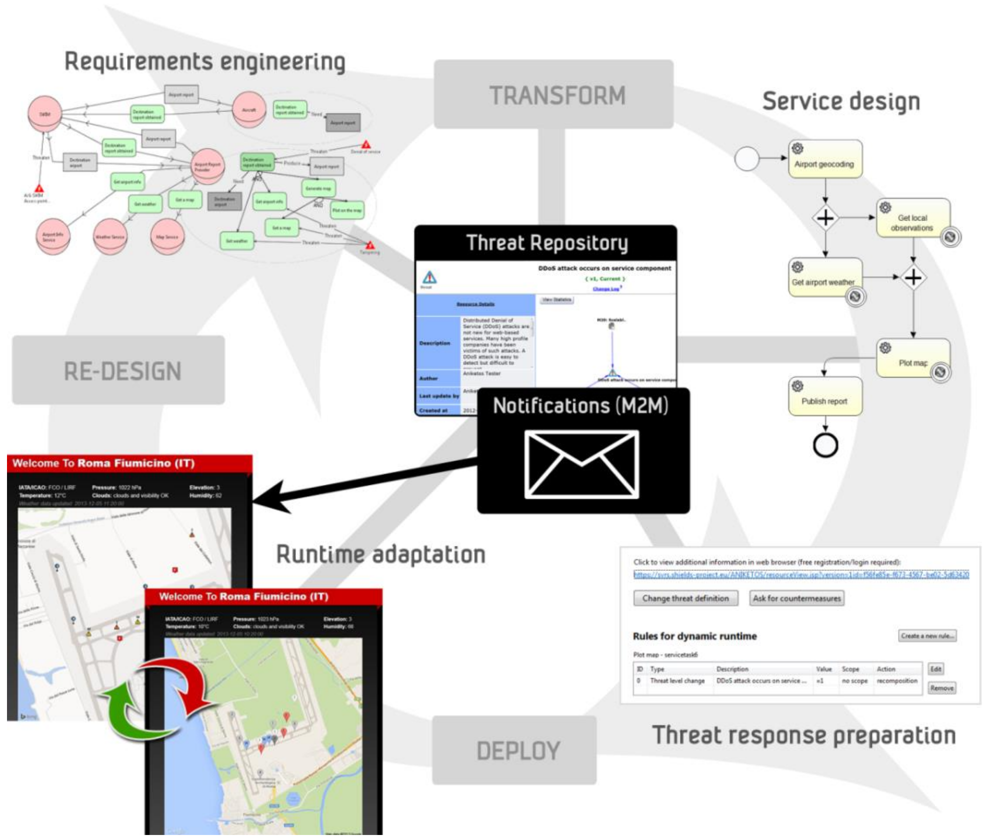
Threats Management Throughout the Software Service Life-Cycle



Click to view additional information in web browser (free registration/login required):

https://svrs.shields-project.eu/ANIKETOS/resourceView.jsp?version=1id=f56fe85e-f673-4567-be02-5d63420

Rules for dynamic runtime

Plot map - servicetask6

ID	Type	Description	Value	Scope	Action
0	Threat level change	DDoS attack occurs on service ...	=1	no scope	recomposition

SINTEF

Erlend Andreas Gjære

and Per Håkon Meland

@erlangsec

ANIKETOS

1st International Workshop on Graphical Models for Security (GraMSec), Grenoble, 12th April 2014

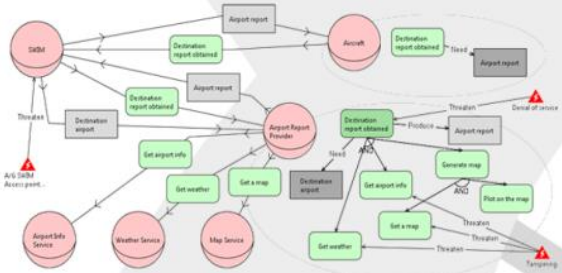
SEVENTH FRAMEWORK PROGRAMME

Overview

Threat modelling for **composite services** to support both **prevention** and **correction**.

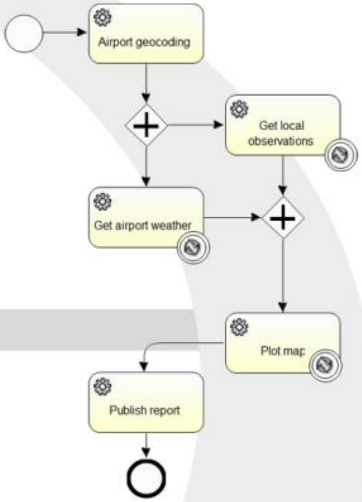
- Goal-oriented modelling (STS-Tool)
- Service process modelling (BPMN)
- Threat repository
- Dynamic adaptation at run-time

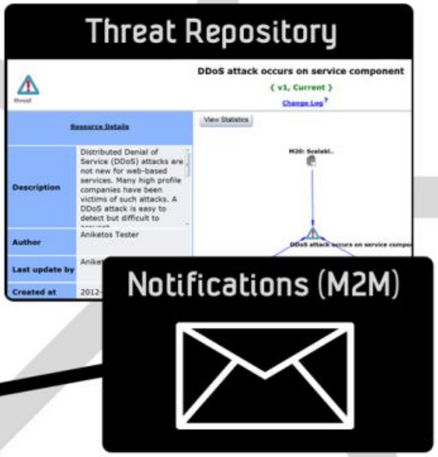
Requirements engineering



TRANSFORM

Service design





Threat Repository

DDoS attack occurs on service component

{ v1, Current }

Change Log

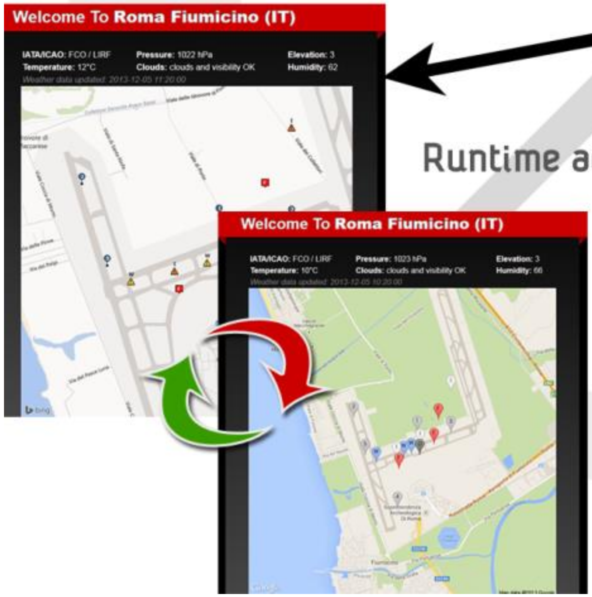
Resource Details

View Statistics

Description	Distributed Denial of Service (DDoS) attacks are not new for web-based services. Many high profile companies have been victims of such attacks. A DDoS attack is easy to detect but difficult to
Author	Aniketos Tester
Last update by	Aniket
Created at	2012-

Notifications (M2M)

RE-DESIGN



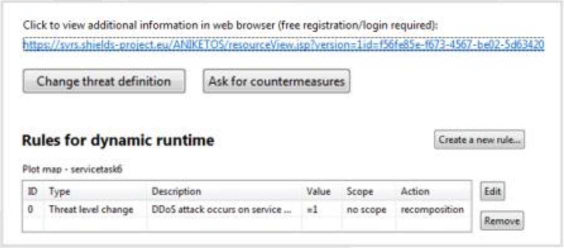
Welcome To **Roma Fiumicino (IT)**

IATA/ICAO: FCO / LIRF **Pressure:** 1022 hPa **Elevation:** 3
Temperature: 12°C **Clouds:** clouds and visibility OK **Humidity:** 62
Weather data updated: 2013-12-05 11:20:00

Welcome To **Roma Fiumicino (IT)**

IATA/ICAO: FCO / LIRF **Pressure:** 1023 hPa **Elevation:** 3
Temperature: 10°C **Clouds:** clouds and visibility OK **Humidity:** 66
Weather data updated: 2013-12-05 10:20:00

Runtime adaptation



Click to view additional information in web browser (free registration/login required):

https://svrs.shields-project.eu/ANIKETOS/resourceView.jsp?version=1id=f56fe85e-f673-4567-be02-5d63420

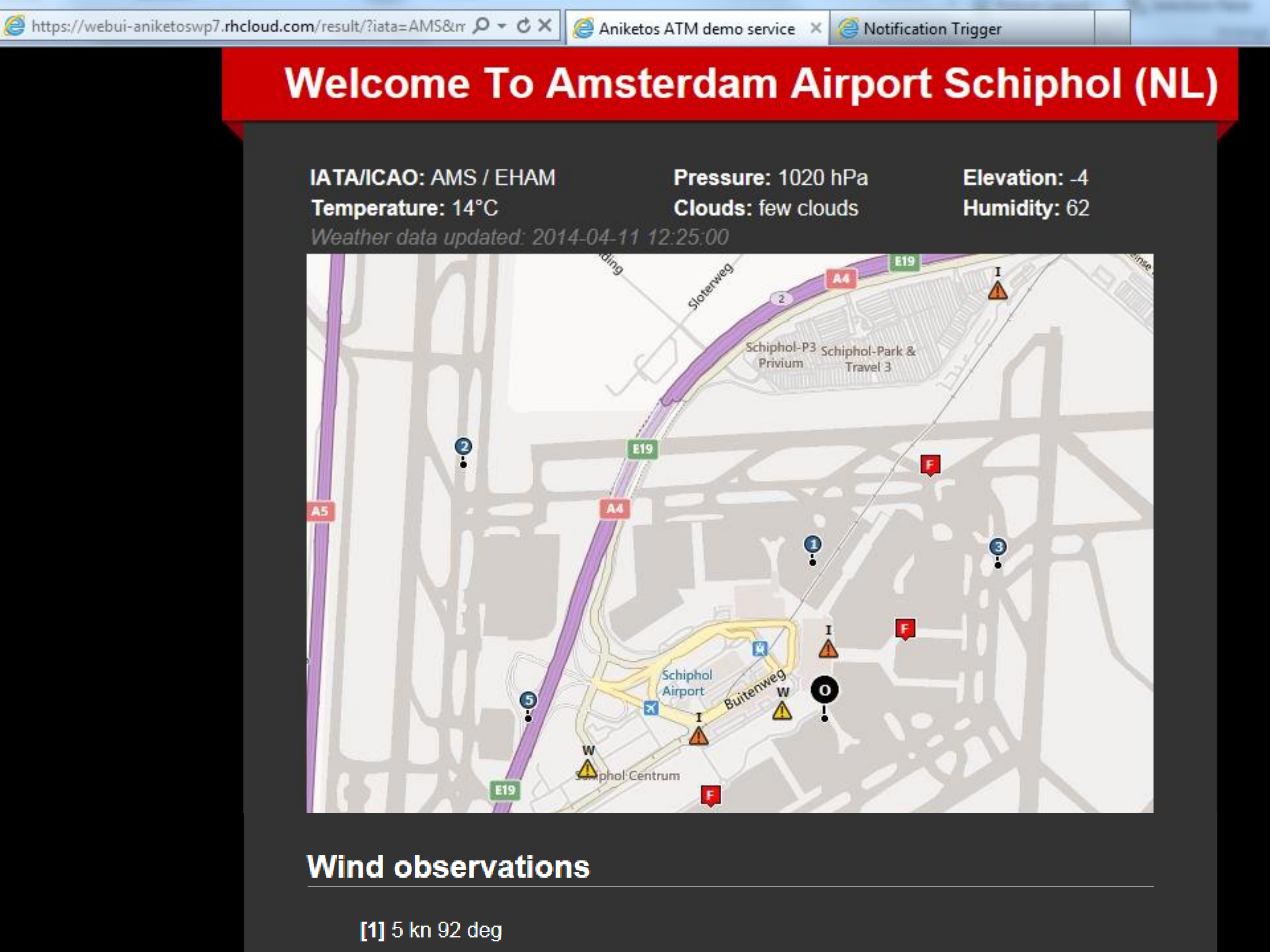
Rules for dynamic runtime

Plot map - servicetask6

ID	Type	Description	Value	Scope	Action
0	Threat level change	DDoS attack occurs on service ...	=1	no scope	recomposition

Threat response preparation

DEPLOY



Welcome To Amsterdam Airport Schiphol (NL)

IATA/ICAO: AMS / EHAM **Pressure:** 1020 hPa **Elevation:** -4

Temperature: 14°C **Clouds:** few clouds **Humidity:** 62

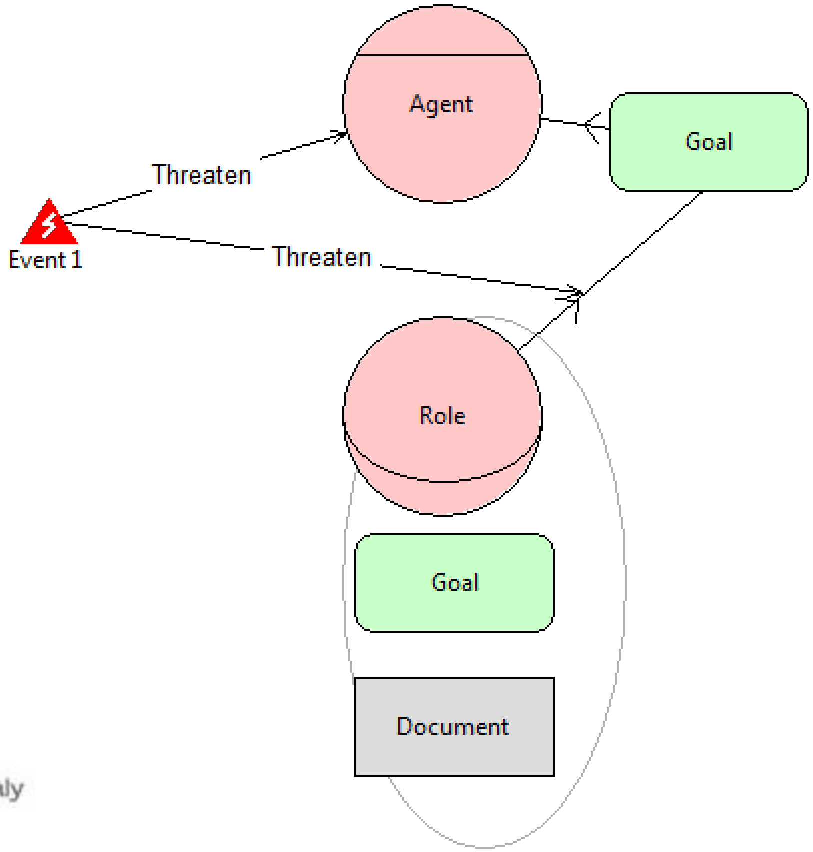
Weather data updated: 2014-04-11 12:25:00

Wind observations

[1] 5 kn 92 deg

Socio-Technical Security Modelling Language and Tool

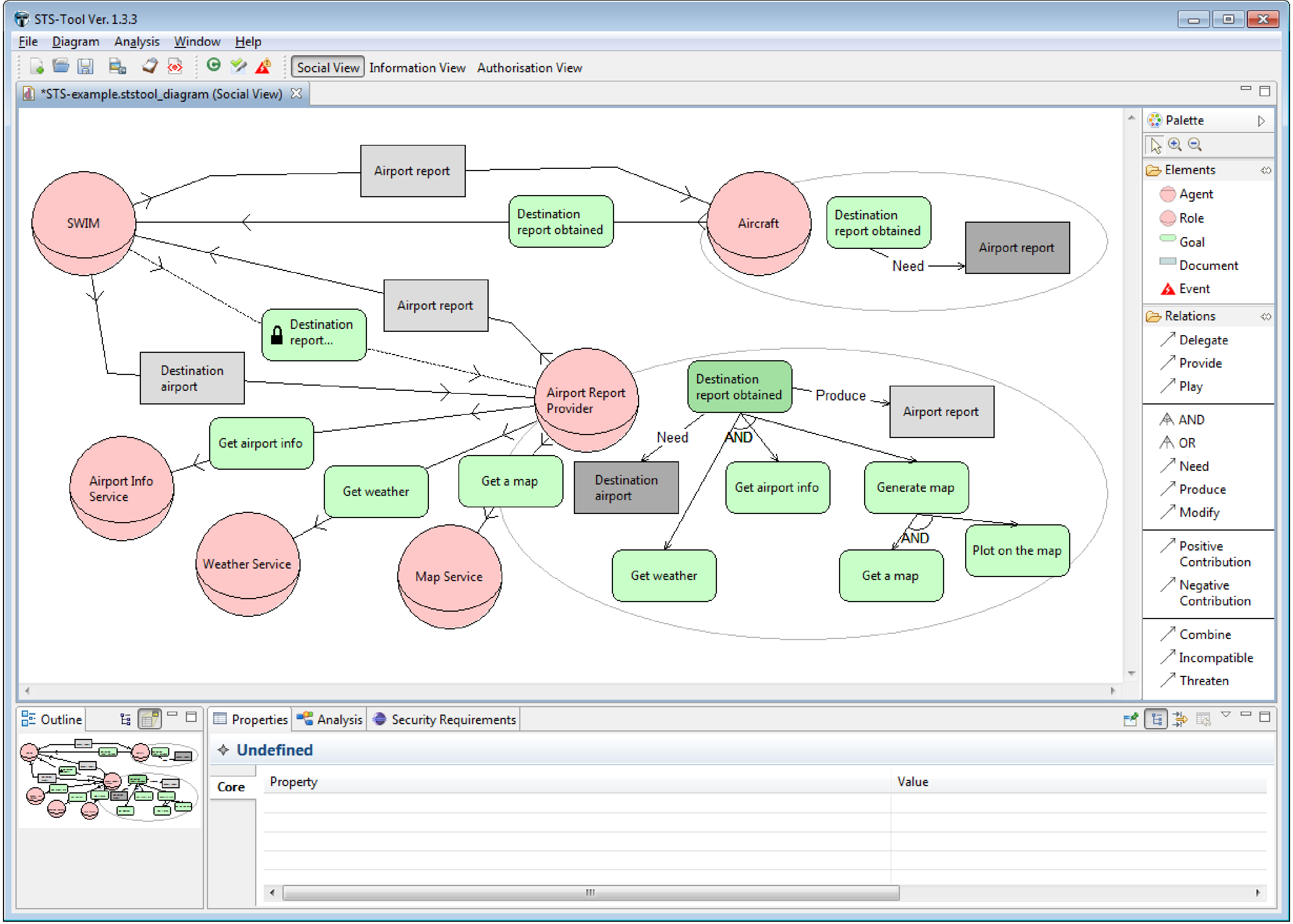
- STS-Tool
  - Graphical representation
  - Consistency/implications analysis
  - Formal requirements output
- Well defined methodology
- Tutorial and free download: www.sts-tool.eu

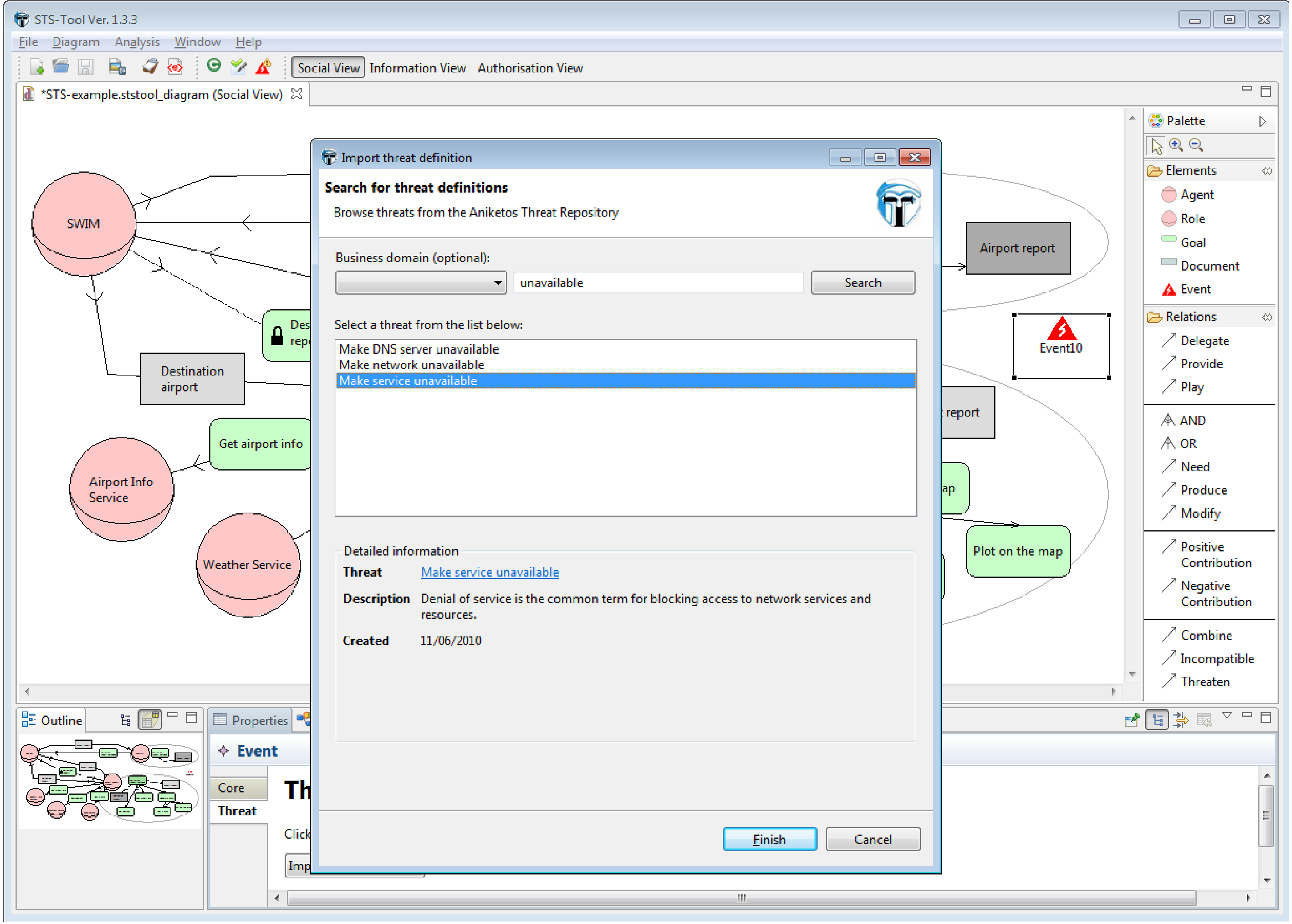


UNIVERSITY OF TRENTO - Italy

Threats in STS-Tool

- Demo…


STS-Tool Ver. 1.3.3
File
Diagram
Analysis
Window
Help
Social View
Information View
Authorisation View
*STS-example.ststool_diagram (Social View)
Airport report
SWIM
Destination report obtained
Aircraft
Destination report obtained
Airport report
Need
Airport report
Destination report...
Destination airport
Airport Report Provider
Destination report obtained
Produce
Airport report
Need
AND
Get airport info
Airport Info Service
Get weather
Get a map
Destination airport
Get airport info
Generate map
AND
Plot on the map
Weather Service
Map Service
Get weather
Get a map
Palette
Elements
Agent
Role
Goal
Document
Event
Relations
Delegate
Provide
Play
AND
OR
Need
Produce
Modify
Positive Contribution
Negative Contribution
Combine
Incompatible
Threaten
Outline
Properties
Analysis
Security Requirements
Undefined
Core
Property
Value



Import threat definition

Search for threat definitions

Browse threats from the Aniketos Threat Repository

Business domain (optional): [ ] unavailable [Search]

Select a threat from the list below:

- Make DNS server unavailable
- Make network unavailable
- Make service unavailable

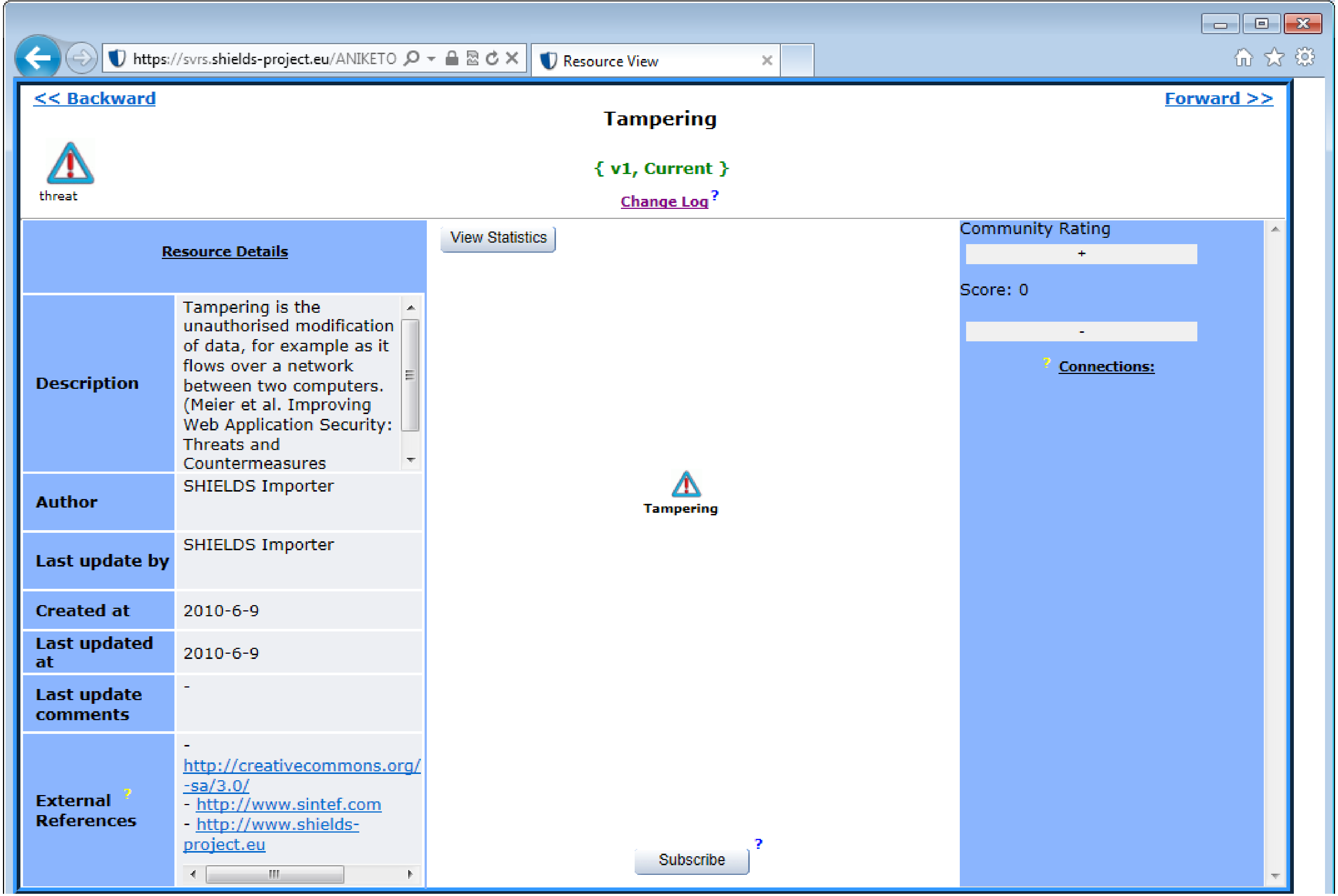
Detailed information

Threat Make service unavailable

Description Denial of service is the common term for blocking access to network services and resources.

Created 11/06/2010

[Finish] [Cancel]



Tampering

{ v1, Current }

Change Log ?

Resource Details

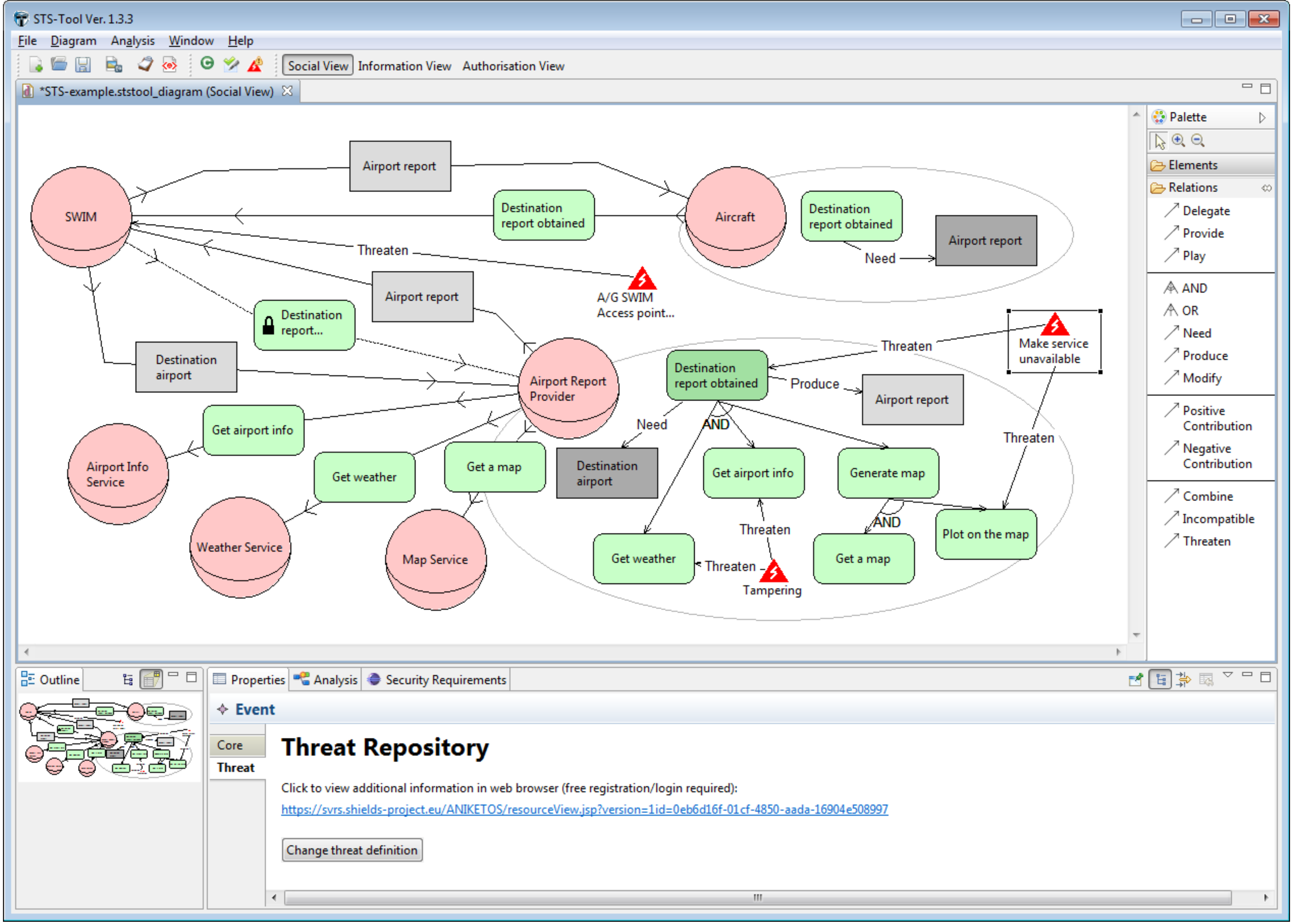
Description	Tampering is the unauthorised modification of data, for example as it flows over a network between two computers. (Meier et al. Improving Web Application Security: Threats and Countermeasures
Author	SHIELDS Importer
Last update by	SHIELDS Importer
Created at	2010-6-9
Last updated at	2010-6-9
Last update comments	-
External ? References	- http://creativecommons.org/ -sa/3.0/ - http://www.sintef.com - http://www.shields-project.eu

Tampering

Community Rating

Score: 0

? Connections:



Event

Threat Repository

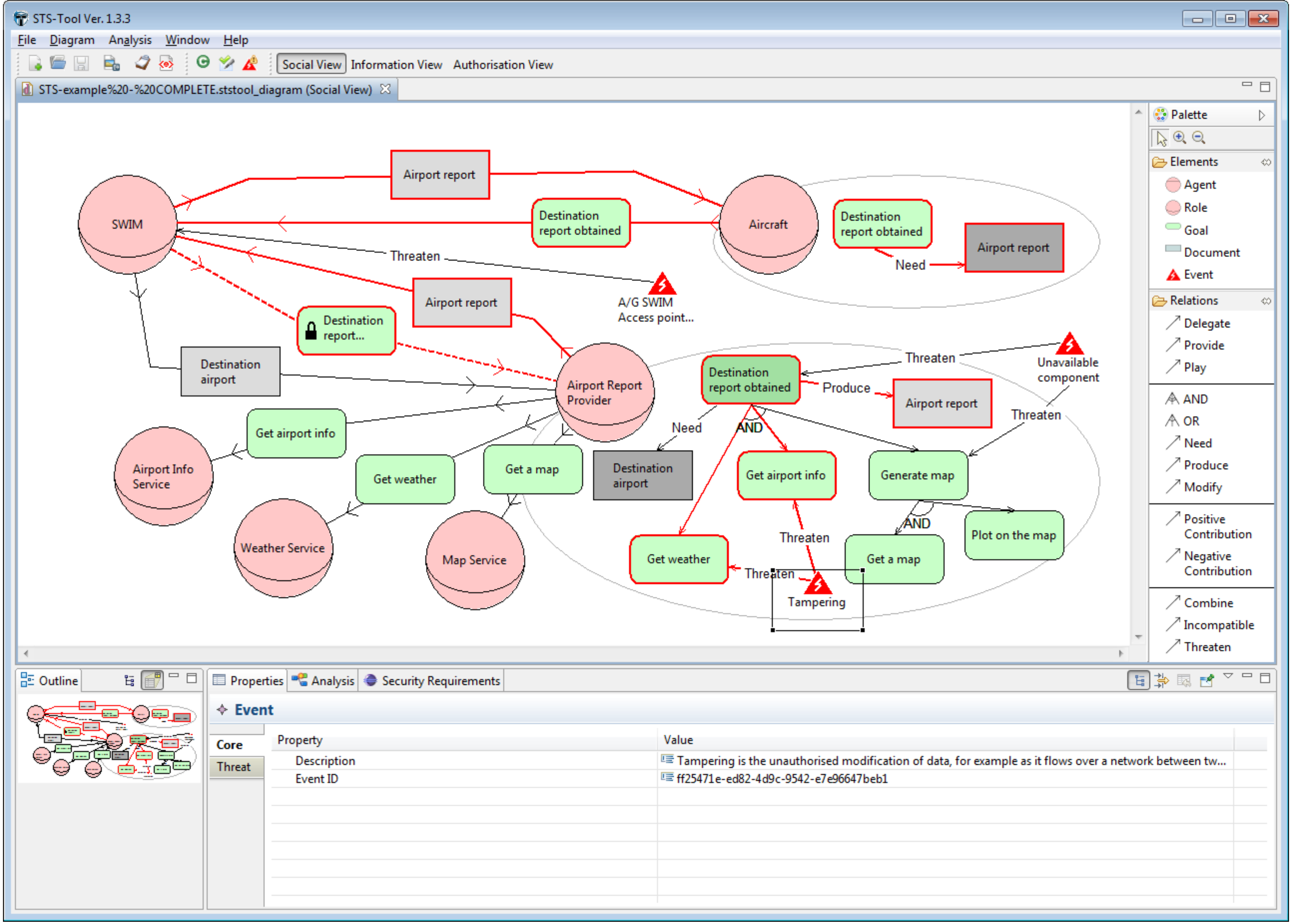
Click to view additional information in web browser (free registration/login required):

https://svrs.shields-project.eu/ANIKETOS/resourceView.jsp?version=1id=0eb6d16f-01cf-4850-aada-16904e508997

Change threat definition

Threat Analysis in STS-Tool

- Demo…



Event

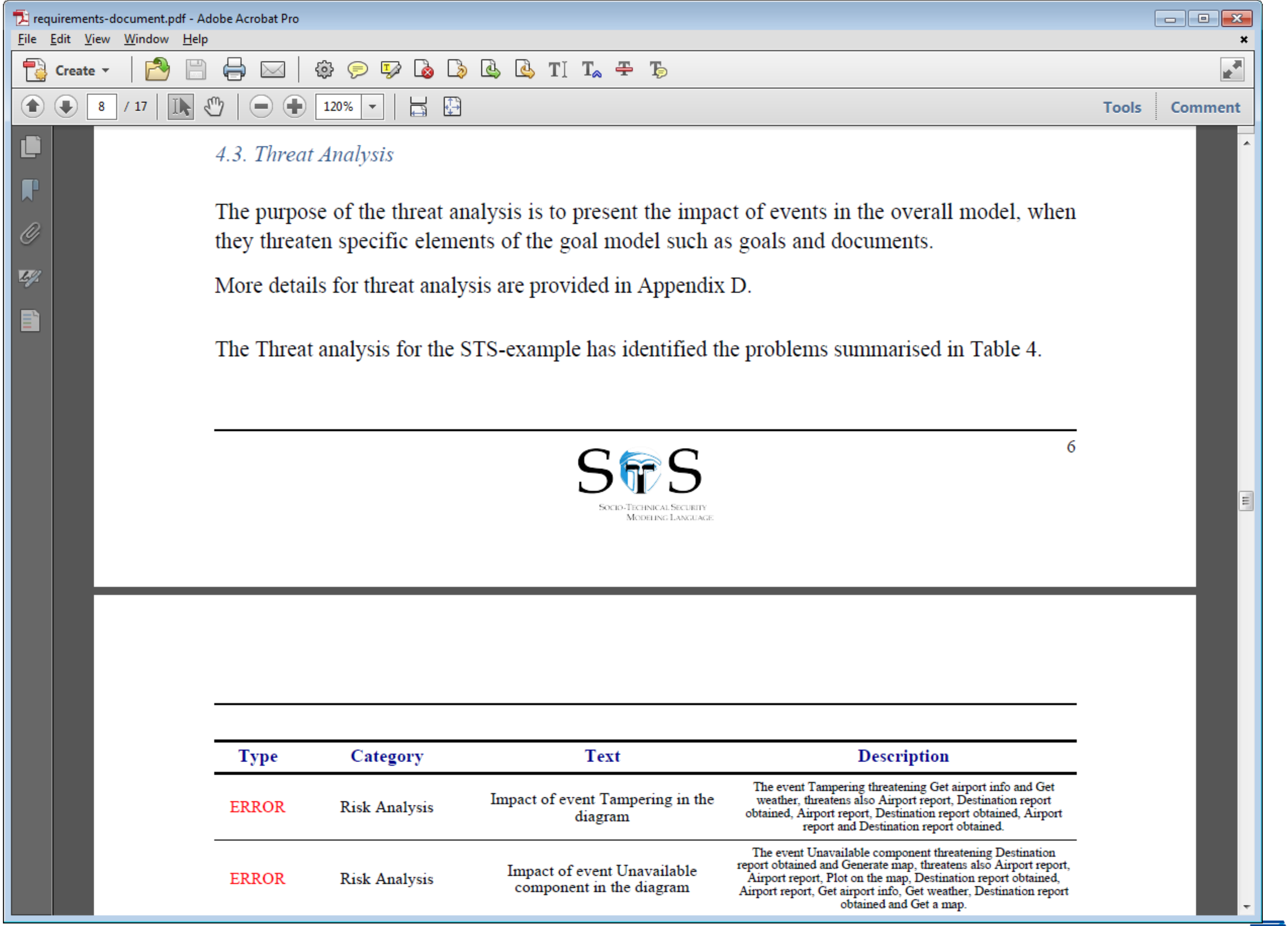
Core

Threat

Property	Value
Description	Tampering is the unauthorised modification of data, for example as it flows over a network between tw...
Event ID	ff25471e-ed82-4d9c-9542-e7e96647beb1

Security Requirements Document with threat analysis

- Demo…



4.3. Threat Analysis

The purpose of the threat analysis is to present the impact of events in the overall model, when they threaten specific elements of the goal model such as goals and documents.

More details for threat analysis are provided in Appendix D.

The Threat analysis for the STS-example has identified the problems summarised in Table 4.

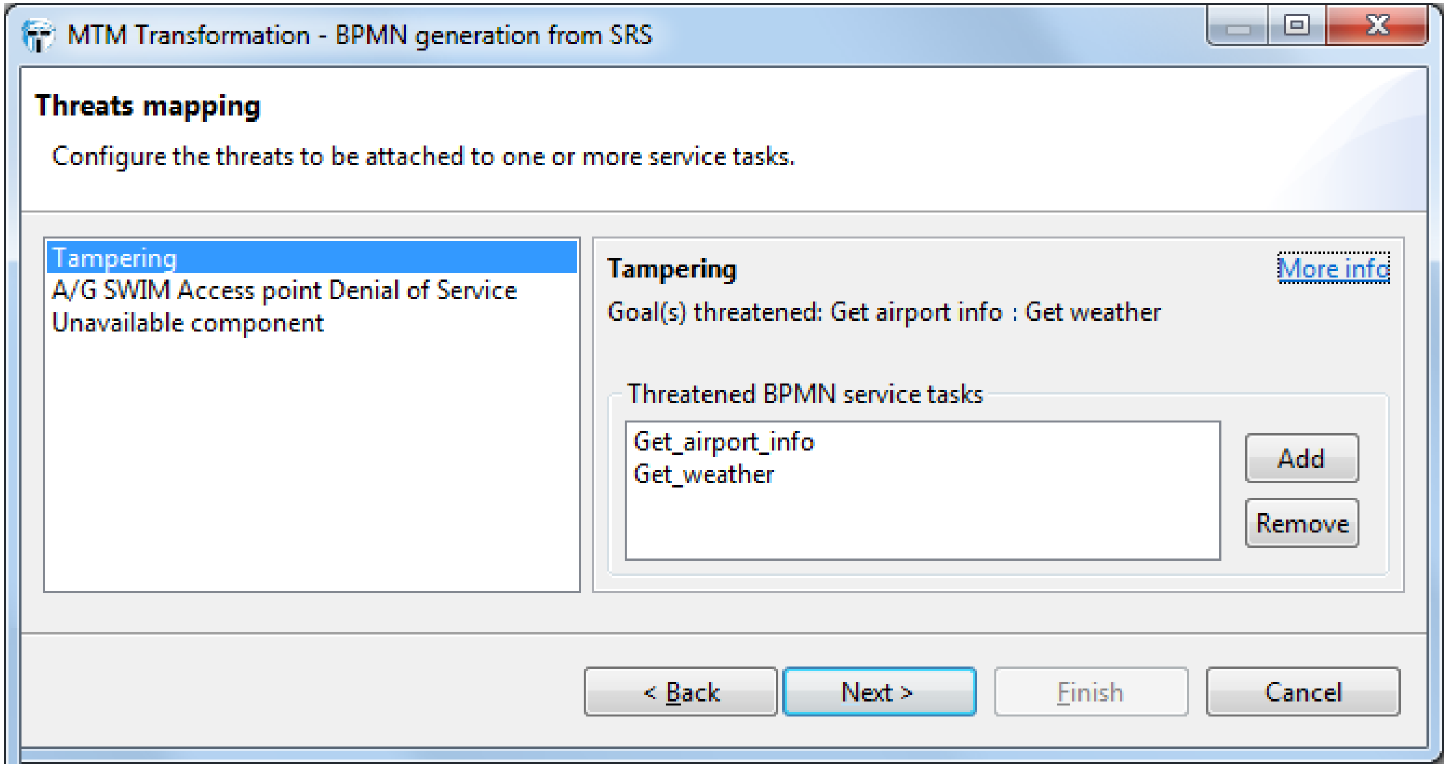
6

STS
Socio-Technical Security
Modeling Language

Type	Category	Text	Description
ERROR	Risk Analysis	Impact of event Tampering in the diagram	The event Tampering threatening Get airport info and Get weather, threatens also Airport report, Destination report obtained, Airport report, Destination report obtained, Airport report and Destination report obtained.
ERROR	Risk Analysis	Impact of event Unavailable component in the diagram	The event Unavailable component threatening Destination report obtained and Generate map, threatens also Airport report, Airport report, Plot on the map, Destination report obtained, Airport report, Get airport info, Get weather, Destination report obtained and Get a map.

Model transformation

- STS → SRS → BPMN



MTM Transformation - BPMN generation from SRS

Threats mapping

Configure the threats to be attached to one or more service tasks.

Tampering
A/G SWIM Access point Denial of Service
Unavailable component

Tampering

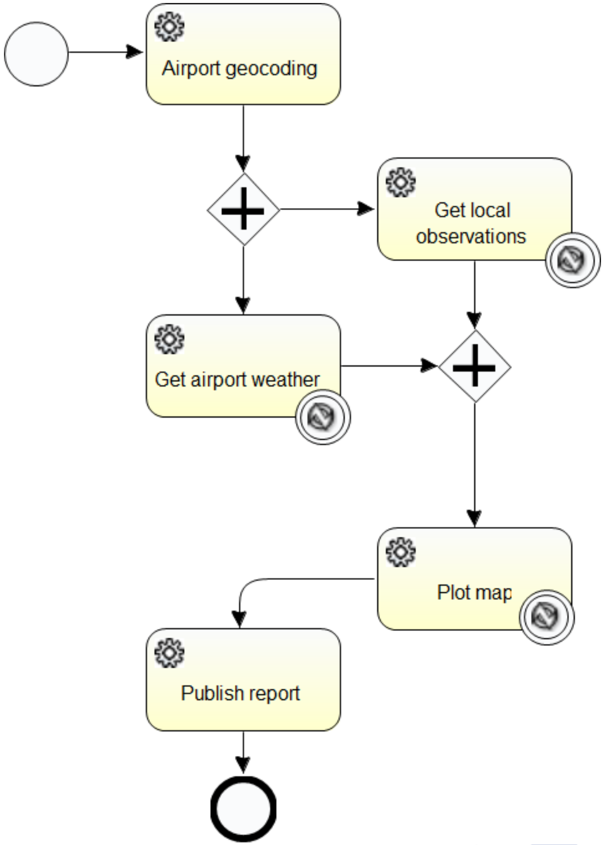
Goal(s) threatened: Get airport info : Get weather

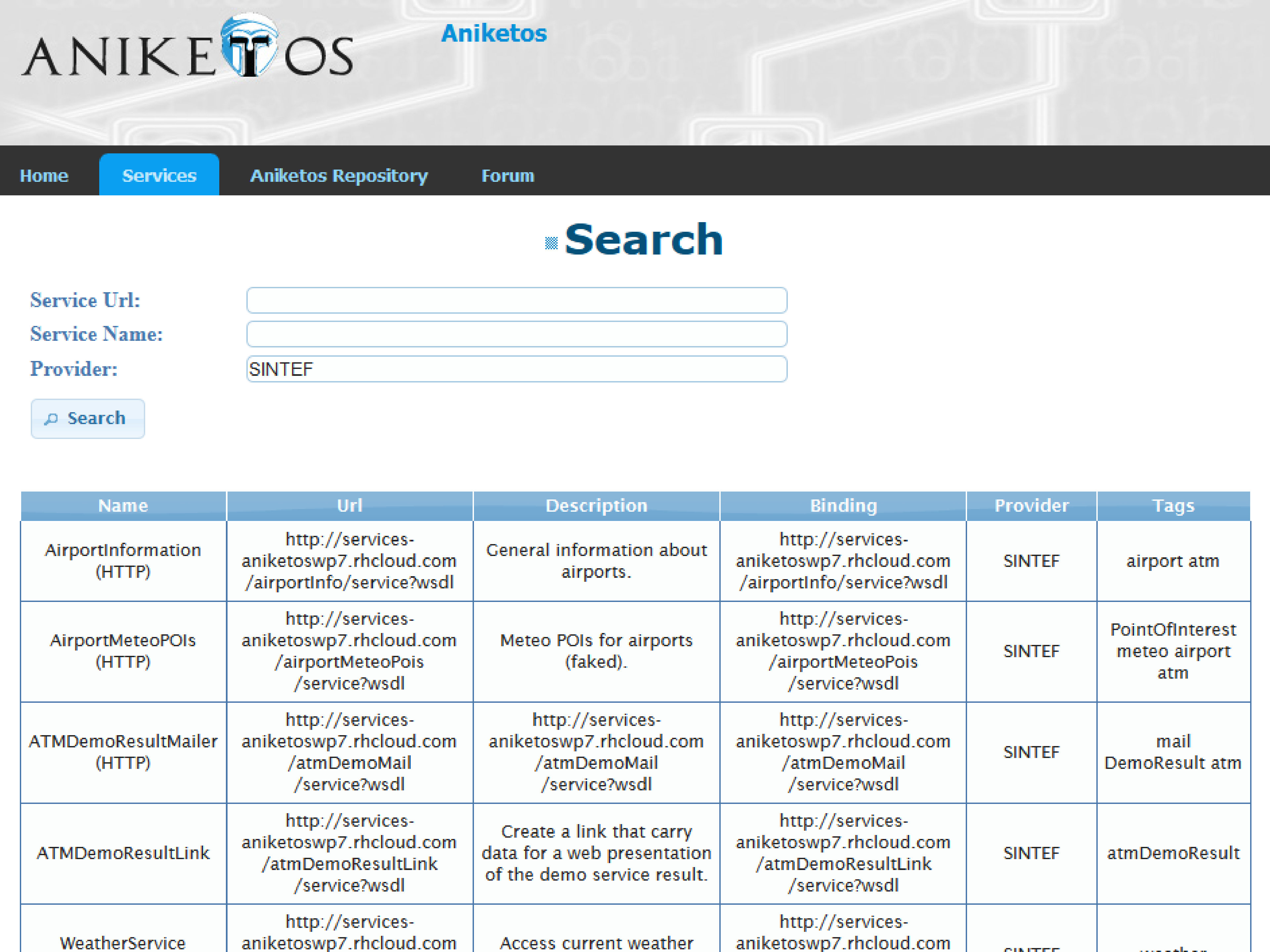
Threatened BPMN service tasks

Get_airport_info
Get_weather

Service Composition Framework

- SCF allows service designers to
  - Specify a service process model (BPMN)
  - Discover services for service tasks
  - Deploy secure composite services
- Extension of Activiti Designer
- HMI for Aniketos security services





Search

Service Url:

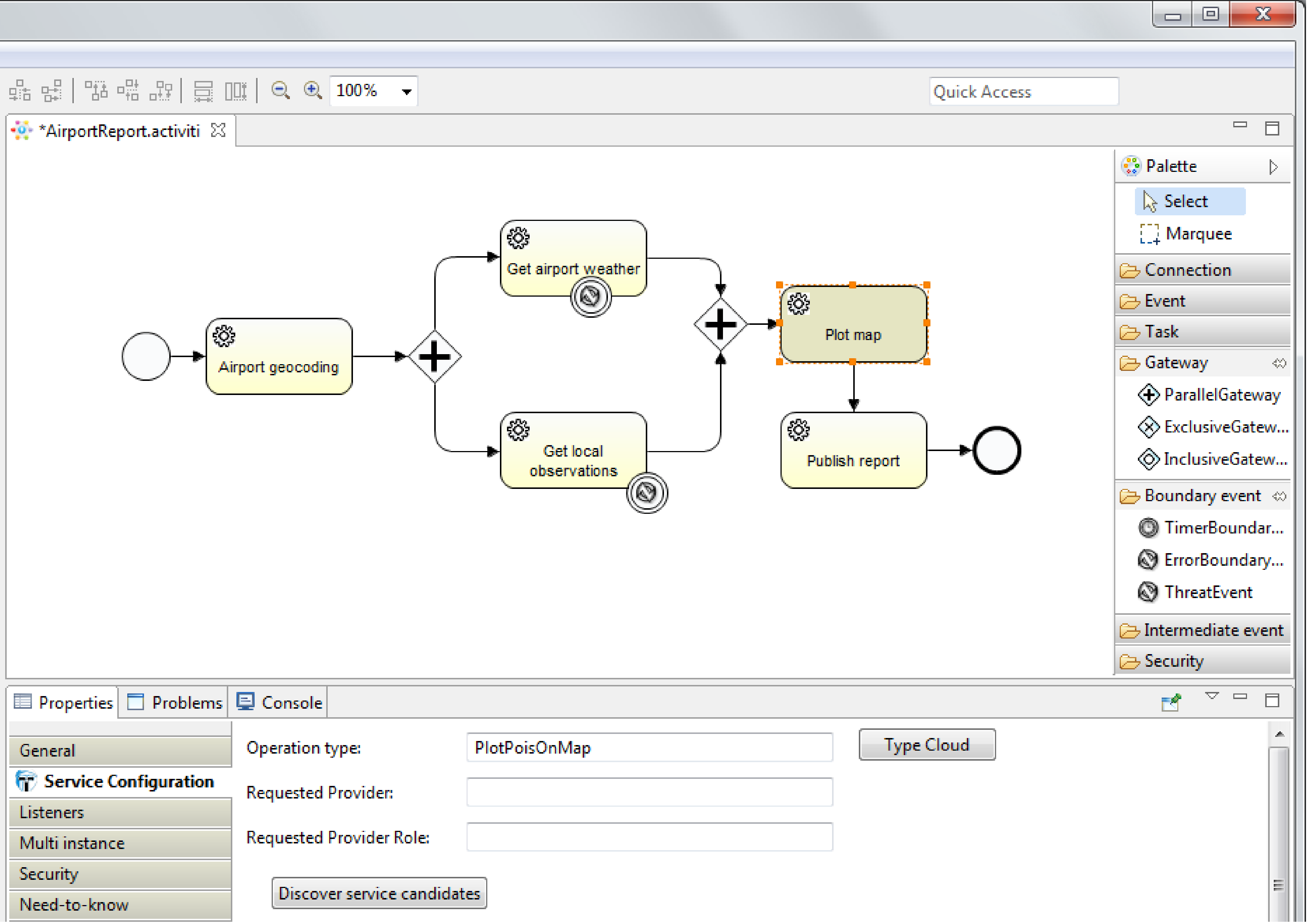
Service Name:

Provider: SINTEF

Name	Url	Description	Binding	Provider	Tags
AirportInformation (HTTP)	http://services-aniketoswp7.rhcloud.com/airportInfo/service?wsdl	General information about airports.	http://services-aniketoswp7.rhcloud.com/airportInfo/service?wsdl	SINTEF	airport atm
AirportMeteoPOIs (HTTP)	http://services-aniketoswp7.rhcloud.com/airportMeteoPois/service?wsdl	Meteo POIs for airports (faked).	http://services-aniketoswp7.rhcloud.com/airportMeteoPois/service?wsdl	SINTEF	PointOfInterest meteo airport atm
ATMDemoResultMailer (HTTP)	http://services-aniketoswp7.rhcloud.com/atmDemoMail/service?wsdl	http://services-aniketoswp7.rhcloud.com/atmDemoMail/service?wsdl	http://services-aniketoswp7.rhcloud.com/atmDemoMail/service?wsdl	SINTEF	mail DemoResult atm
ATMDemoResultLink	http://services-aniketoswp7.rhcloud.com/atmDemoResultLink/service?wsdl	Create a link that carry data for a web presentation of the demo service result.	http://services-aniketoswp7.rhcloud.com/atmDemoResultLink/service?wsdl	SINTEF	atmDemoResult
WeatherService	http://services-aniketoswp7.rhcloud.com	Access current weather	http://services-aniketoswp7.rhcloud.com	SINTEF	weather

Threats in SCF

- Demo…



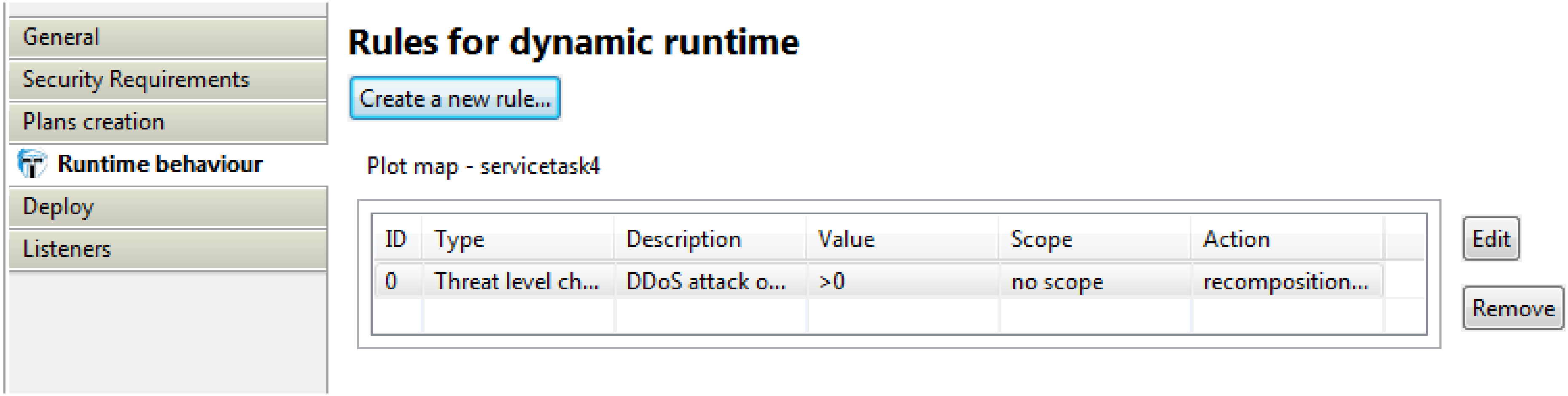
Operation type: PlotPoisOnMap

Requested Provider:

Requested Provider Role:

Prepare dynamic runtime

- Demo…

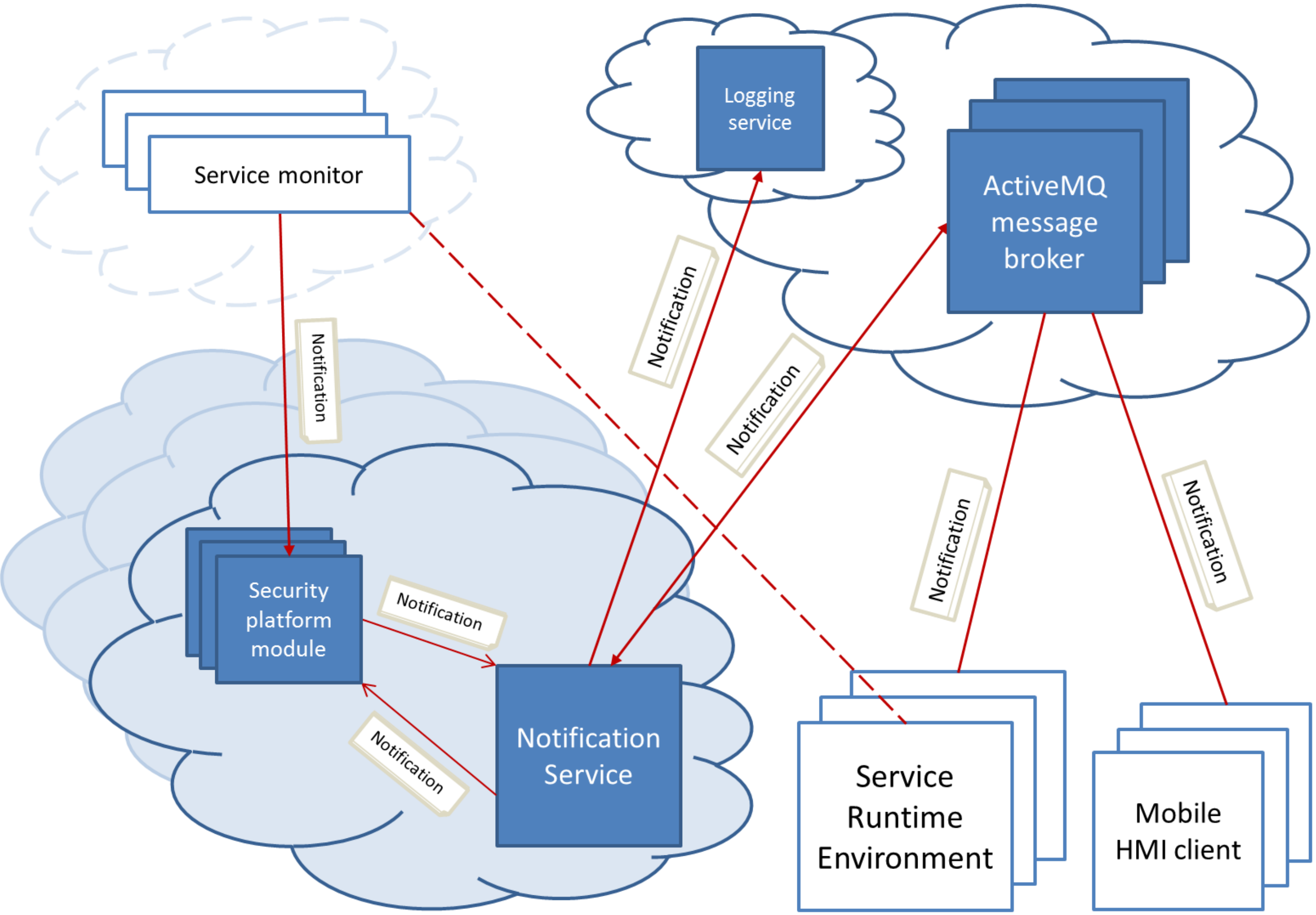


Rules for dynamic runtime

Plot map - servicetask4

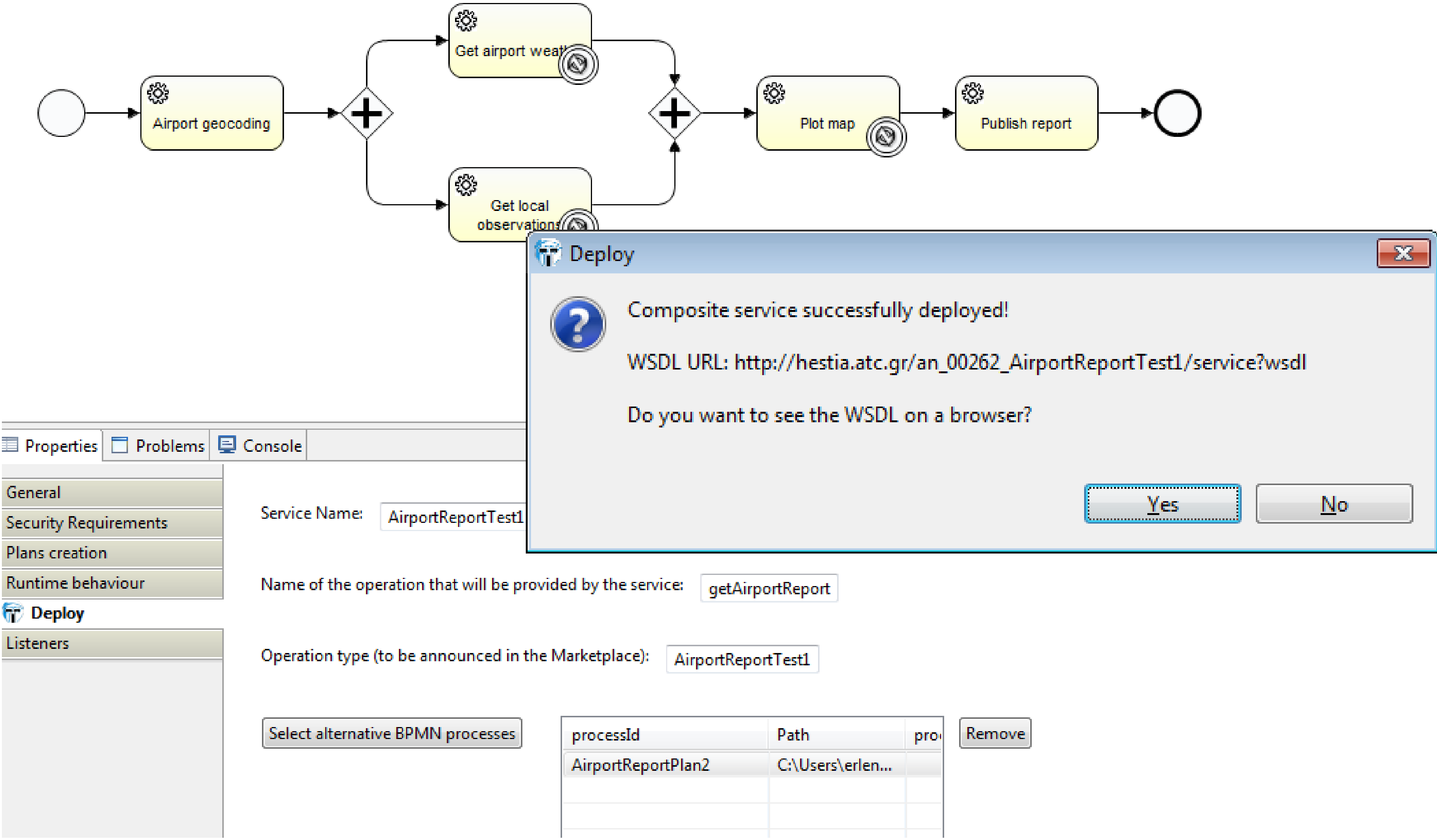
ID	Type	Description	Value	Scope	Action
0	Threat level ch...	DDoS attack o...	>0	no scope	recomposition...

Security Monitoring and Notification



Deployment

- Demo…



Composite service successfully deployed!

WSDL URL: http://hestia.atc.gr/an_00262_AirportReportTest1/service?wsdl

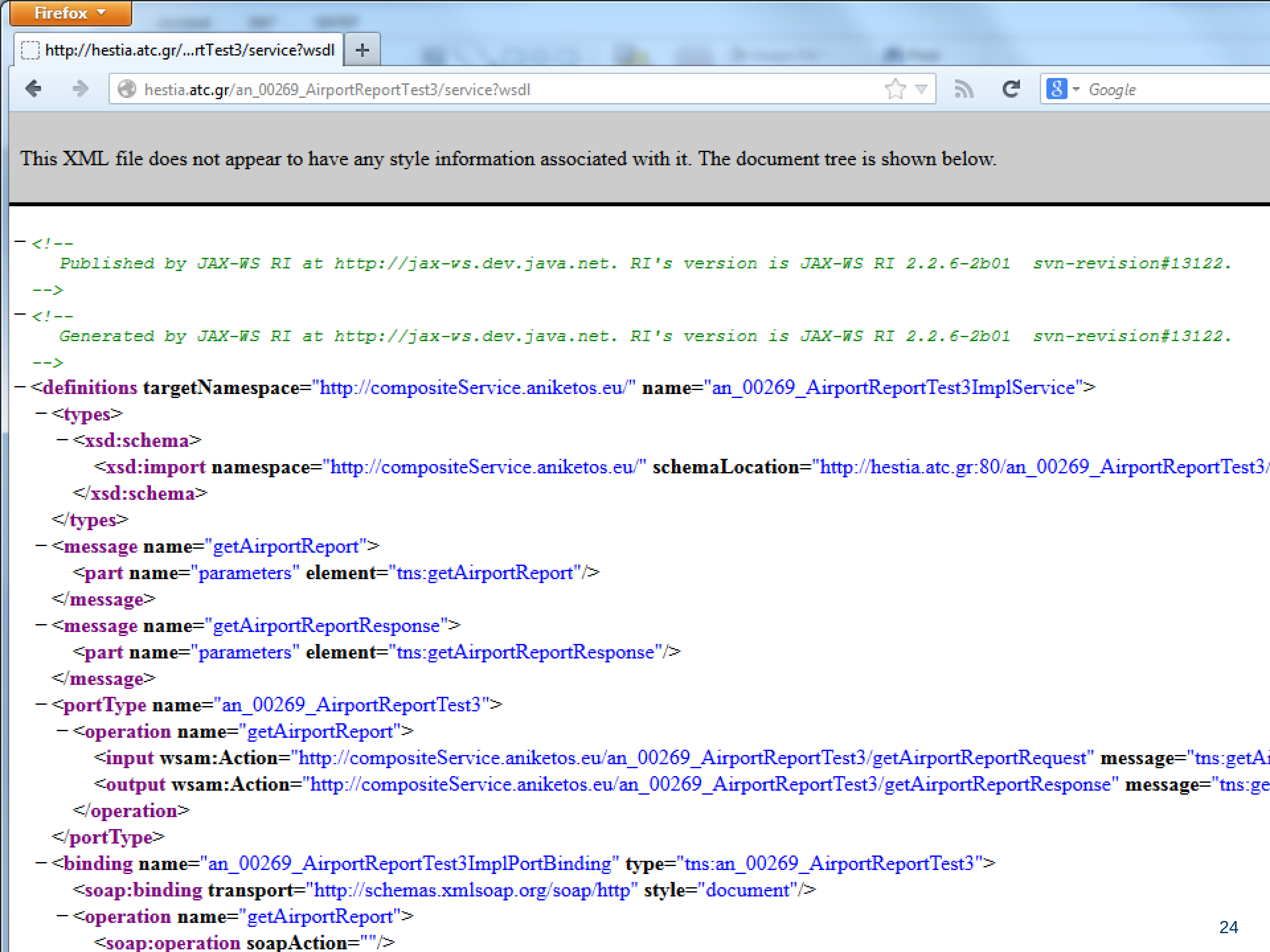
Do you want to see the WSDL on a browser?

Service Name: AirportReportTest1

Name of the operation that will be provided by the service: getAirportReport

Operation type (to be announced in the Marketplace): AirportReportTest1

processId	Path	pro
AirportReportPlan2	C:\Users\erlen...	

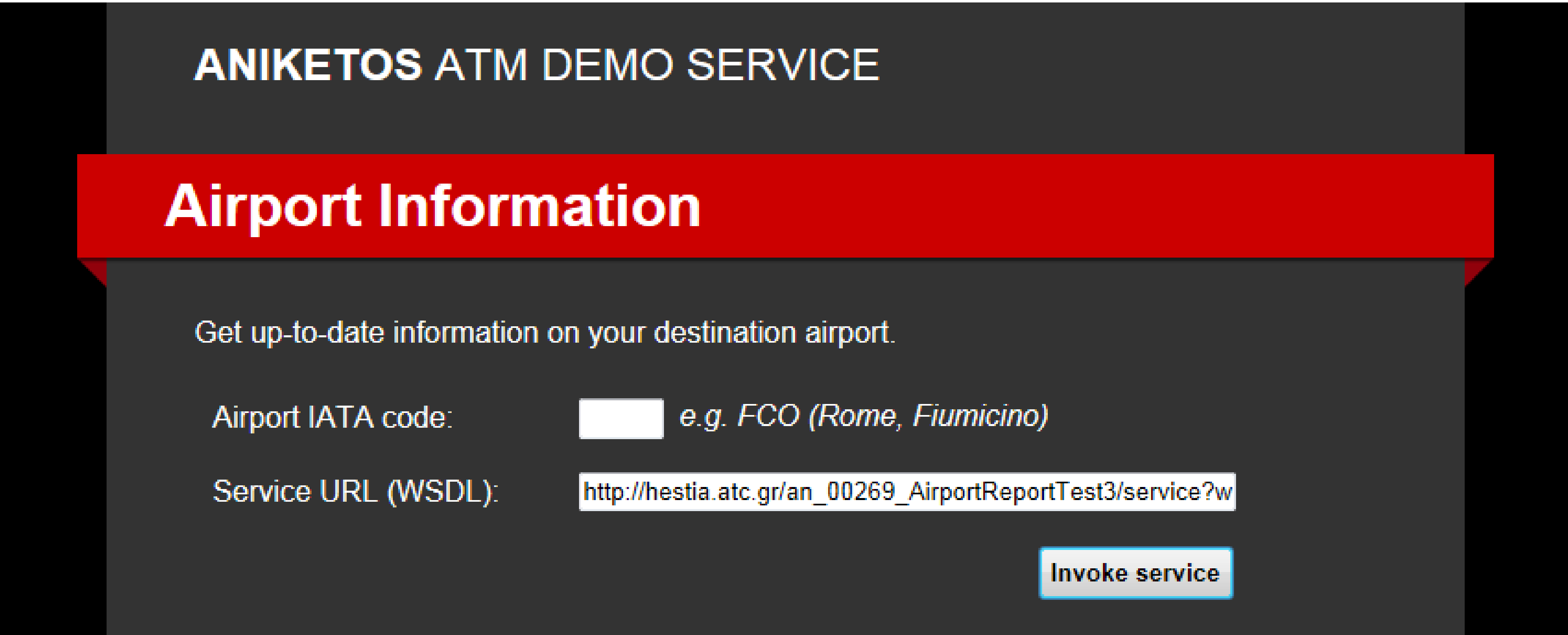

Firefox
http://hestia.atc.gr/...rtTest3/service?wsdl
hestia.atc.gr/an_00269_AirportReportTest3/service?wsdl
Google

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
– <!--
    Published by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is JAX-WS RI 2.2.6-2b01  svn-revision#13122.
  -->
– <!--
    Generated by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is JAX-WS RI 2.2.6-2b01  svn-revision#13122.
  -->
– <definitions targetNamespace="http://compositeService.aniketos.eu/" name="an_00269_AirportReportTest3ImplService">
  – <types>
    – <xsd:schema>
        <xsd:import namespace="http://compositeService.aniketos.eu/" schemaLocation="http://hestia.atc.gr:80/an_00269_AirportReportTest3/
      </xsd:schema>
    </types>
  – <message name="getAirportReport">
      <part name="parameters" element="tns:getAirportReport"/>
    </message>
  – <message name="getAirportReportResponse">
      <part name="parameters" element="tns:getAirportReportResponse"/>
    </message>
  – <portType name="an_00269_AirportReportTest3">
    – <operation name="getAirportReport">
        <input wsam:Action="http://compositeService.aniketos.eu/an_00269_AirportReportTest3/getAirportReportRequest" message="tns:getAi
        <output wsam:Action="http://compositeService.aniketos.eu/an_00269_AirportReportTest3/getAirportReportResponse" message="tns:ge
      </operation>
    </portType>
  – <binding name="an_00269_AirportReportTest3ImplPortBinding" type="tns:an_00269_AirportReportTest3">
      <soap:binding transport="http://schemas.xmlsoap.org/soap/http" style="document"/>
    – <operation name="getAirportReport">
        <soap:operation soapAction=""/>
```

Dynamic adaptation of service

- Runtime demo..
  - http://bit.ly/AniketosATMdemo



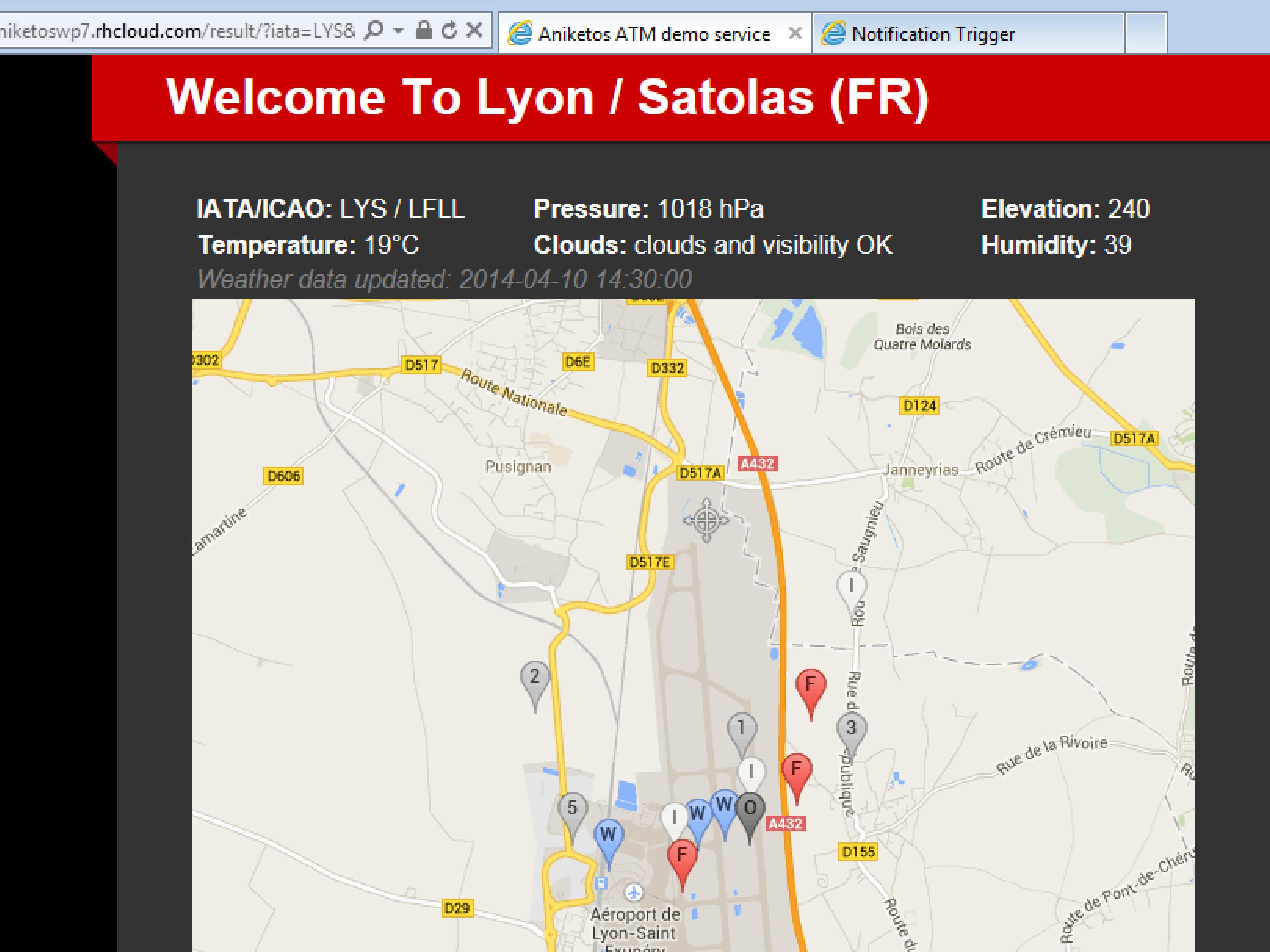
ANIKETOS ATM DEMO SERVICE

Airport Information

Get up-to-date information on your destination airport.

Airport IATA code: e.g. FCO (Rome, Fiumicino)

Service URL (WSDL): http://hestia.atc.gr/an_00269_AirportReportTest3/service?w

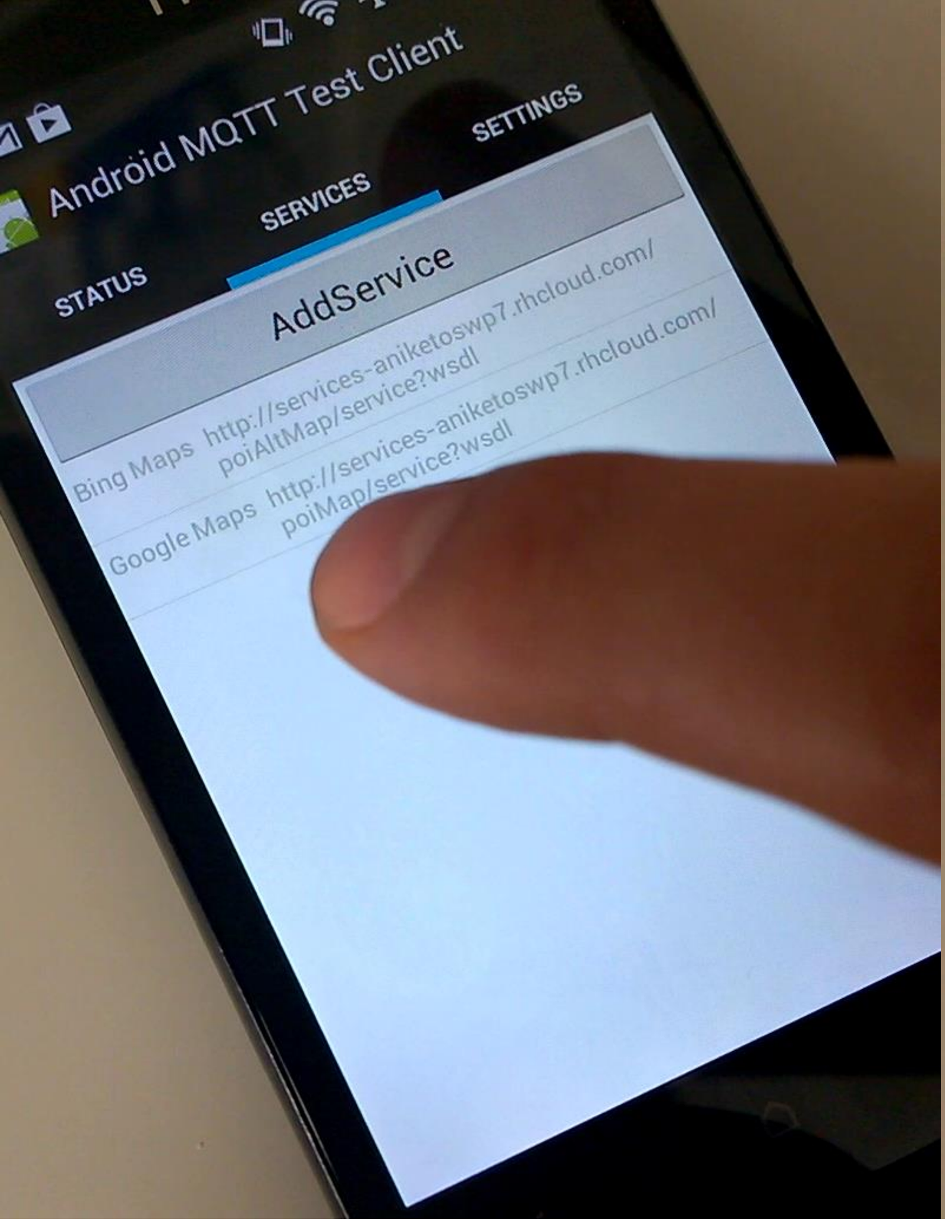

niketoswp7.rhcloud.com/result/?iata=LYS&
Aniketos ATM demo service
Notification Trigger

Welcome To Lyon / Satolas (FR)

IATA/ICAO: LYS / LFLL **Pressure:** 1018 hPa **Elevation:** 240

Temperature: 19°C **Clouds:** clouds and visibility OK **Humidity:** 39

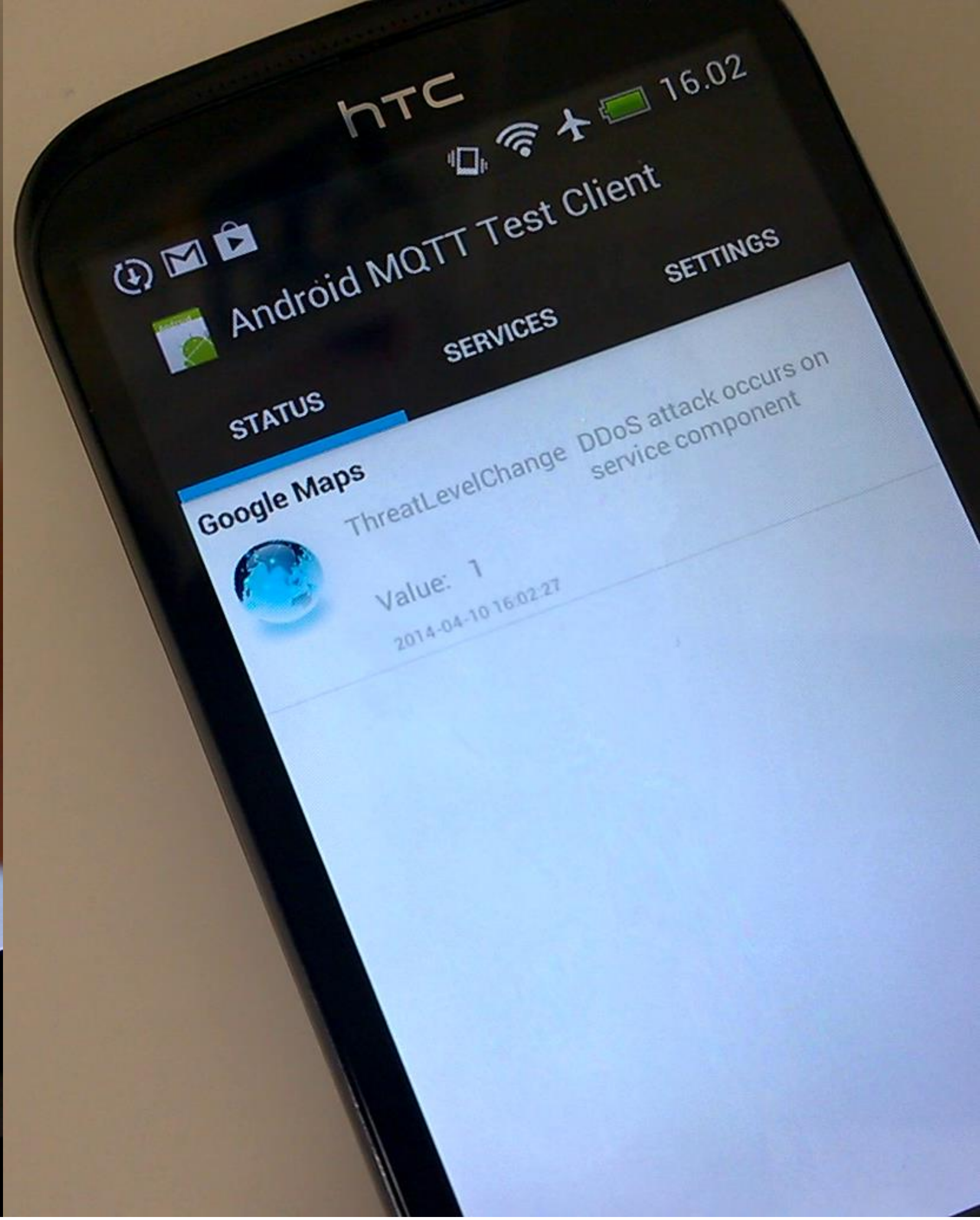
Weather data updated: 2014-04-10 14:30:00



AddService

Bing Maps http://services-aniketoswp7.rhcloud.com/poiAltMap/service?wsdl

Google Maps http://services-aniketoswp7.rhcloud.com/poiMap/service?wsdl

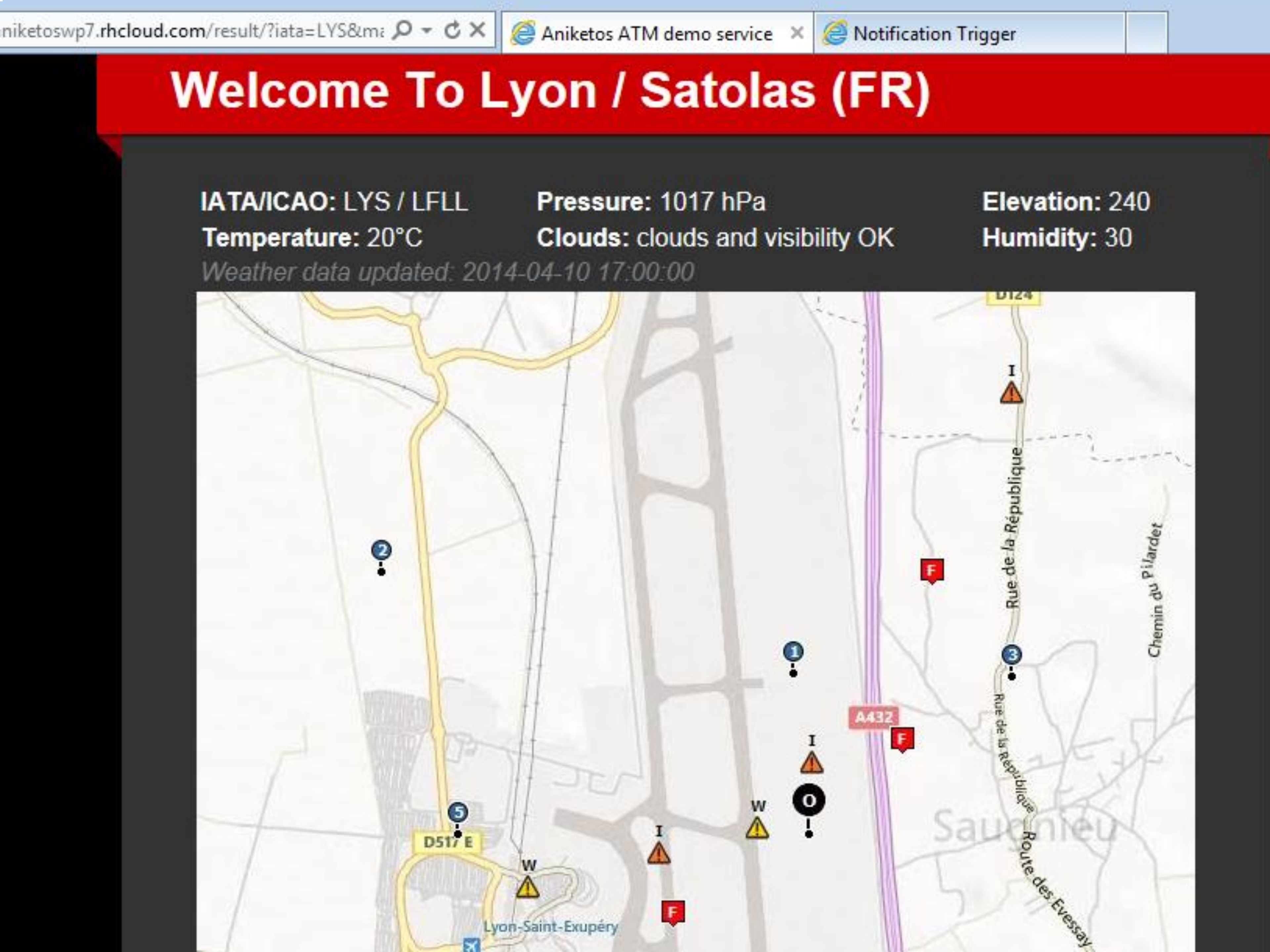


Google Maps

ThreatLevelChange DDoS attack occurs on service component

Value: 1

2014-04-10 16:02:27



Welcome To Lyon / Satolas (FR)

IATA/ICAO: LYS / LFLL **Pressure:** 1017 hPa **Elevation:** 240

Temperature: 20°C **Clouds:** clouds and visibility OK **Humidity:** 30

Weather data updated: 2014-04-10 17:00:00

Wrap-up

- Threat modelling **is not** risk analysis
- Threats **can be** used for:
  - Expressing/analysing *why* security is needed
  - Defining *triggering points* for run-time adaptation
  - Improved security collaboration with business domain experts(?)

Questions/feedback?

- Erlend Andreas Gjære

  erlendandreas.gjare@sintef.no

  @erlangsec

Software resources:

github.com/AniketosEU

ANIKETOS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant no 257930 (Aniketos).

SEVENTH FRAMEWORK PROGRAMME