

# DAT

---

DECISION AID TOOL FOR CI OPERATORS

**Michał Choraś**

[michal.choras@itti.com.pl](mailto:michal.choras@itti.com.pl)

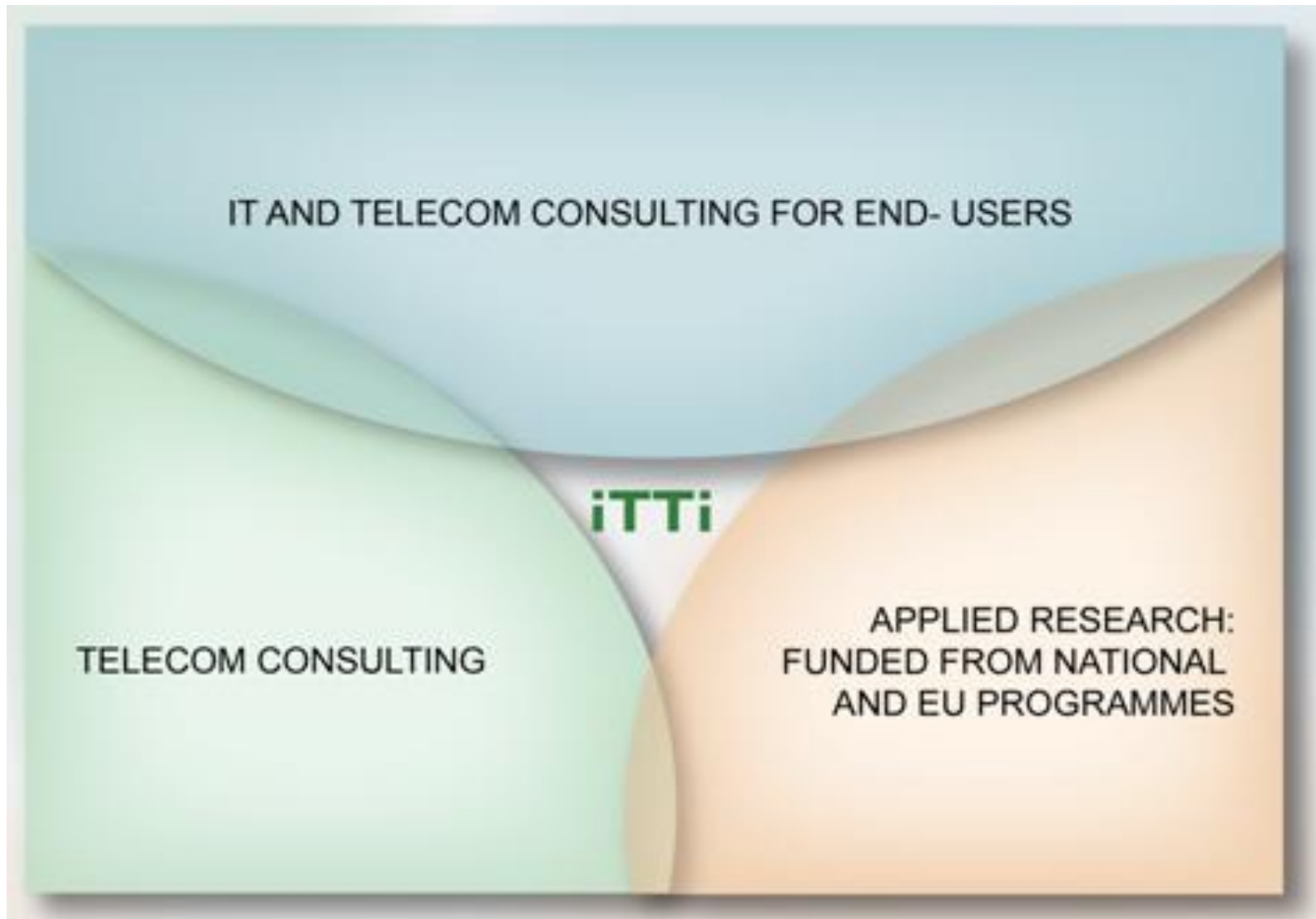
**Rafał Kozik**

[rafal.kozik@itti.com.pl](mailto:rafal.kozik@itti.com.pl)

# Facts and figures (1)



- **company founded in 1996**
- **continuation of the consulting activities of the Franco-Polish School of New Information and Communication Technologies, EFP (1992-96)**
- **since 2003 close co-operation with newly established Division of Applied Informatics at Adam Mickiewicz University**
- **employment: around 60 employees**
- **turnover in 2009: 1,9 ME**
- **fully owned by ITTI partners**



- ITTI consultants poses the following certificates:

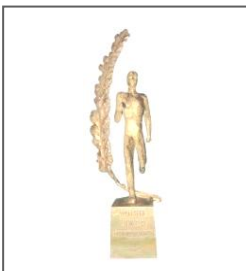


- PRINCE2 Certificate (Projects IN Controlled Environments)
- ITIL Foundation Certificate (IT Service Management Best Practices)
- BS 7799 Certificate (Security)
- TOGAF 8



- Prizes and rewards:

- „Cristal Brussels Prize 2006 and 2010” for the most active and successful Polish SME participating in FP6 and FP7
- Leader of entrepreneurship in Wielkopolska region (2008)
- Prize for innovation in IT appliance given by Polish IT Association (2009)
- Reward for the high performance in R&D projects for European Defence Agency given by Polish Ministry of Defence (2009)



# DAT - objectives



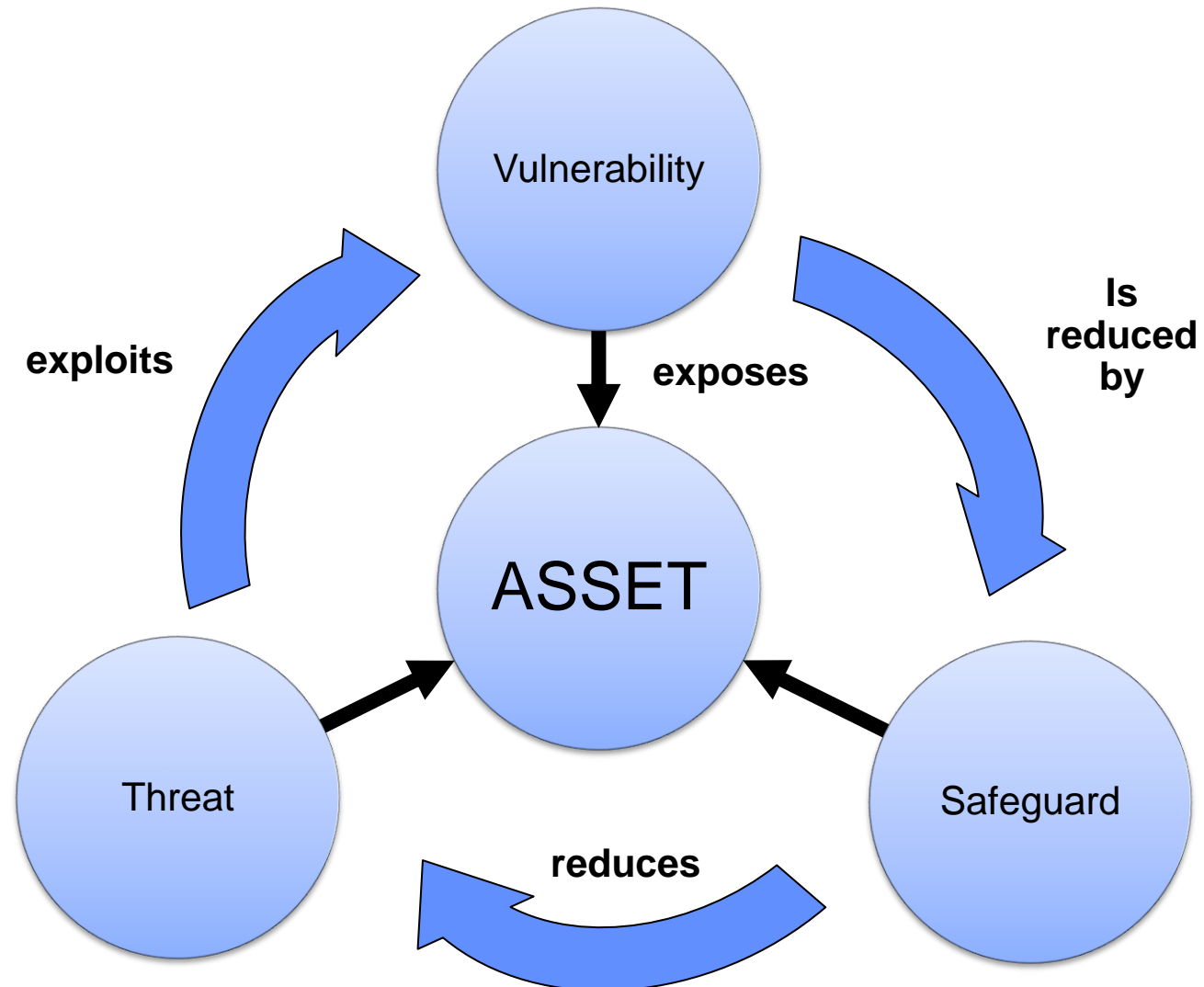
- **INSPIRE Decision Aid Tool (DAT) is intended to be used in industrial SCADA environments for security status evaluation/assessment**
- **Dedicated for security operators**
- **INSPIRE Decision Aid Tool:**
  - **Ranks threats to SCADA network**
  - **Proposes solutions/countermeasures**
  - **Visualizes topology (local/global view)**
  - **Manages:**
    - **Knowledge (the ontological description of system)**
    - **Security Rules**

# DAT - input information

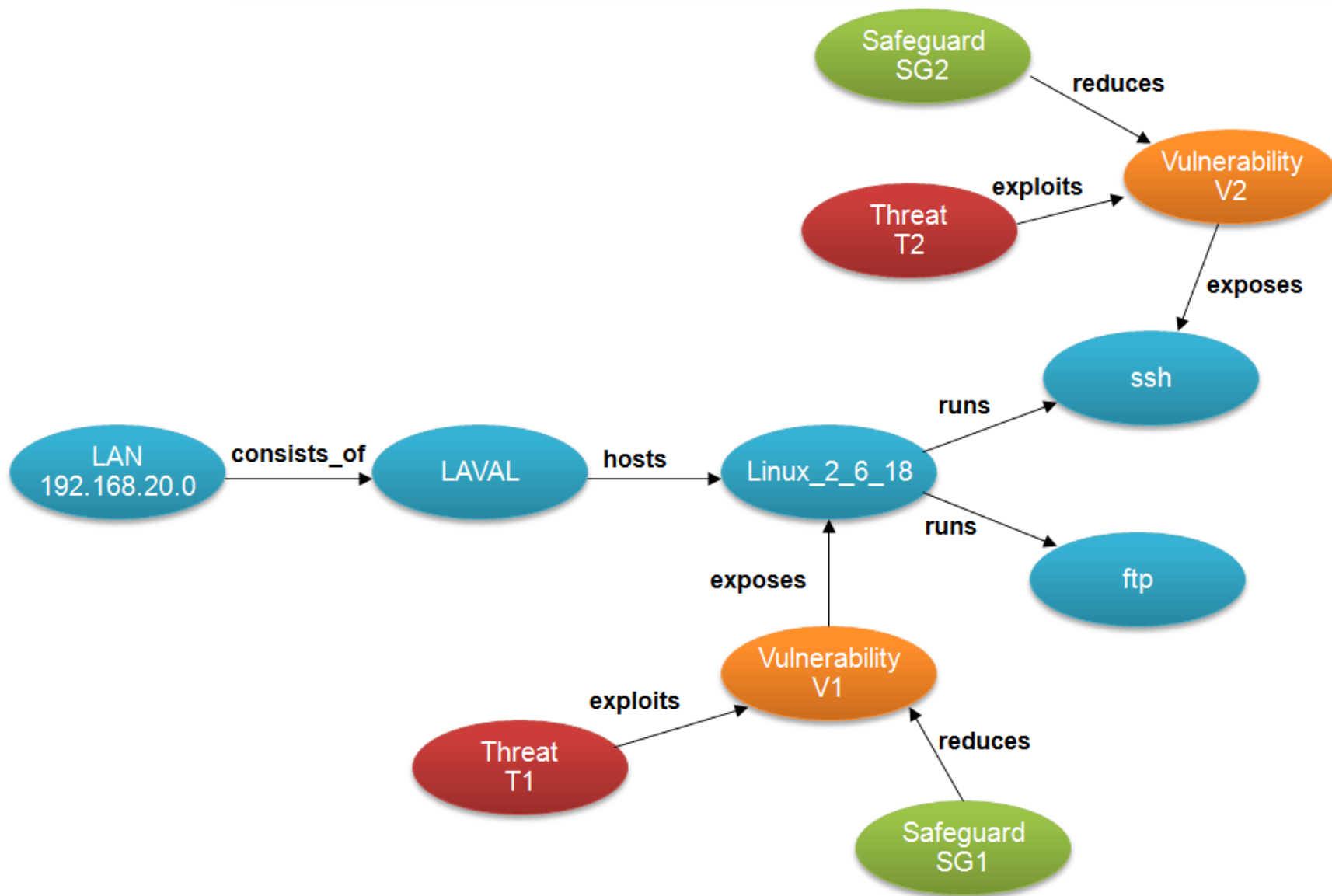


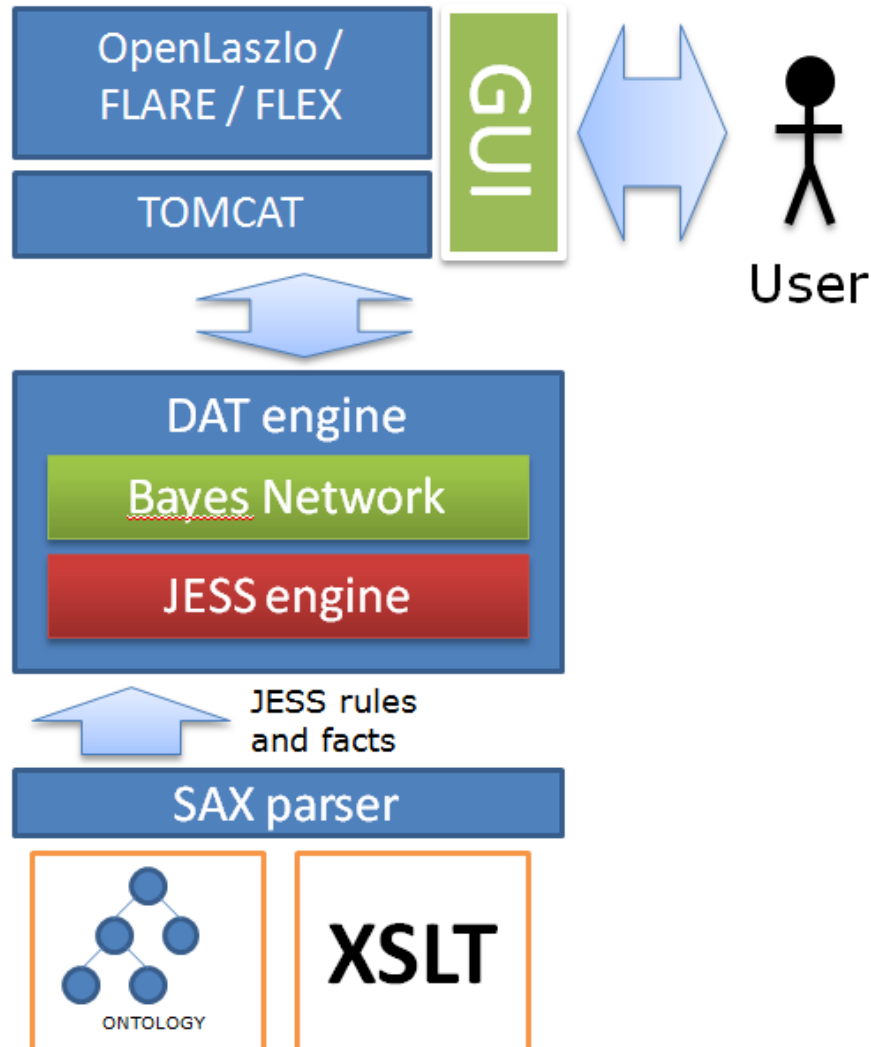
- **ontology – contains i) instances and classes that identify vulnerabilities, threats, attacks which exploit these vulnerabilities and ii) safeguards that reduce threats**
- **topology - describes interconnections between asset instances and is required to perform successful vulnerability identification.**
- **expert rules – provides tool with additional expert knowledge that does not exist in ontology**

# Security Ontology

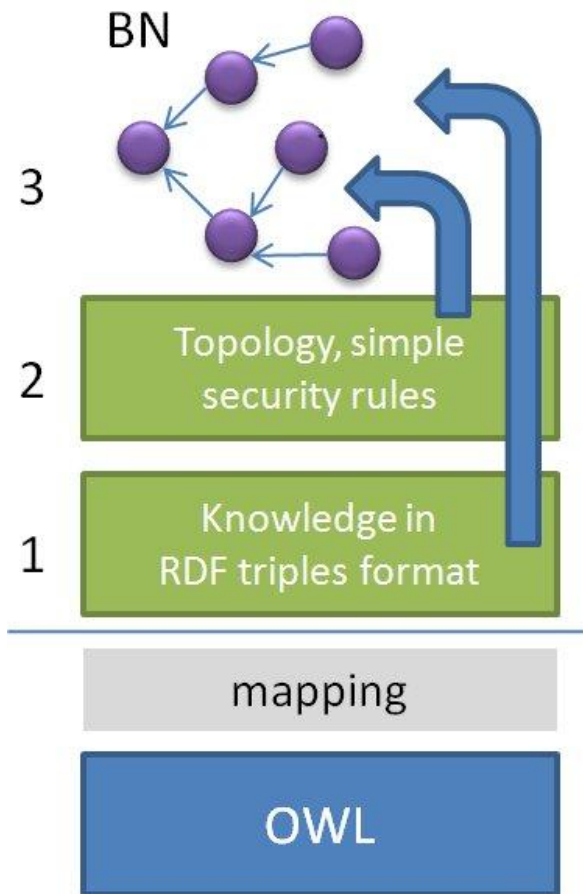


# Security Ontology

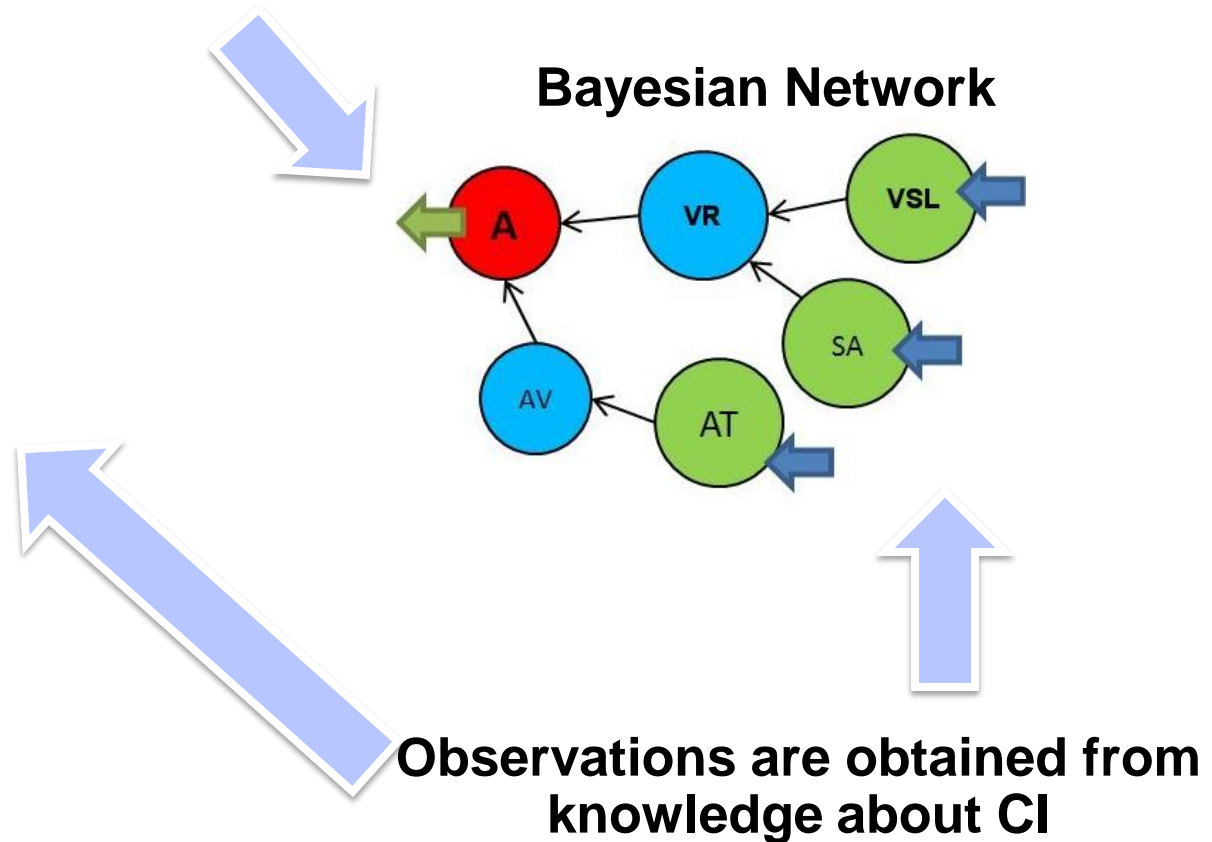




1. OWL ontology file is mapped to format acceptable by JESS using the XSLT transform sheet
2. JESS loads the ontology as JESS facts and rules
3. DAT uses JESS to analyze the topology find threats, vulnerabilities, safeguards and other information
4. DAT uses BN to rank the threats and to asses the risk
5. Tomcat server allows the user to interact with DAT via user-friendly GUI



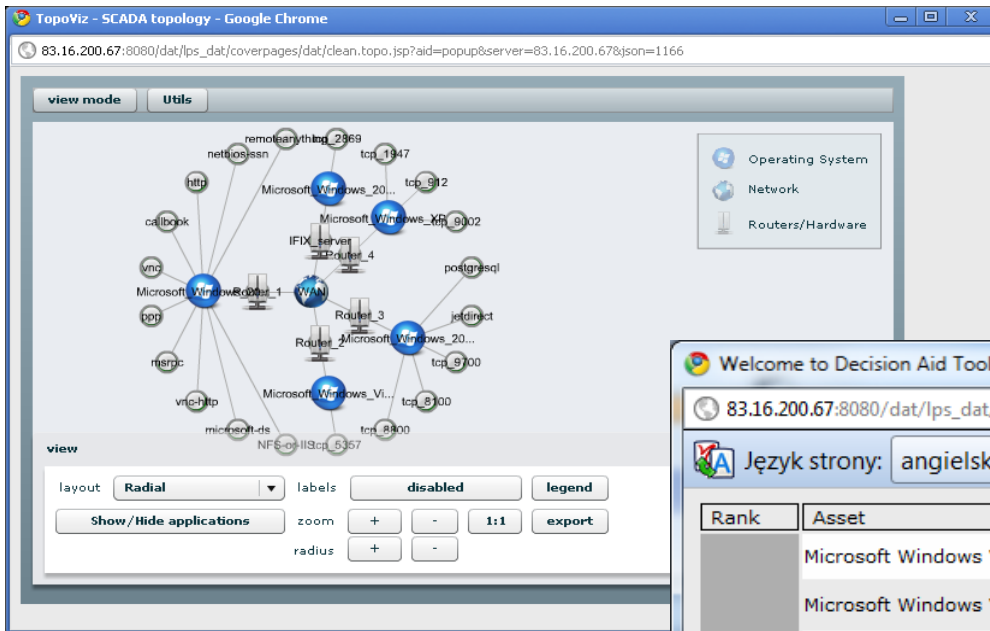
Probability of attack given the observations



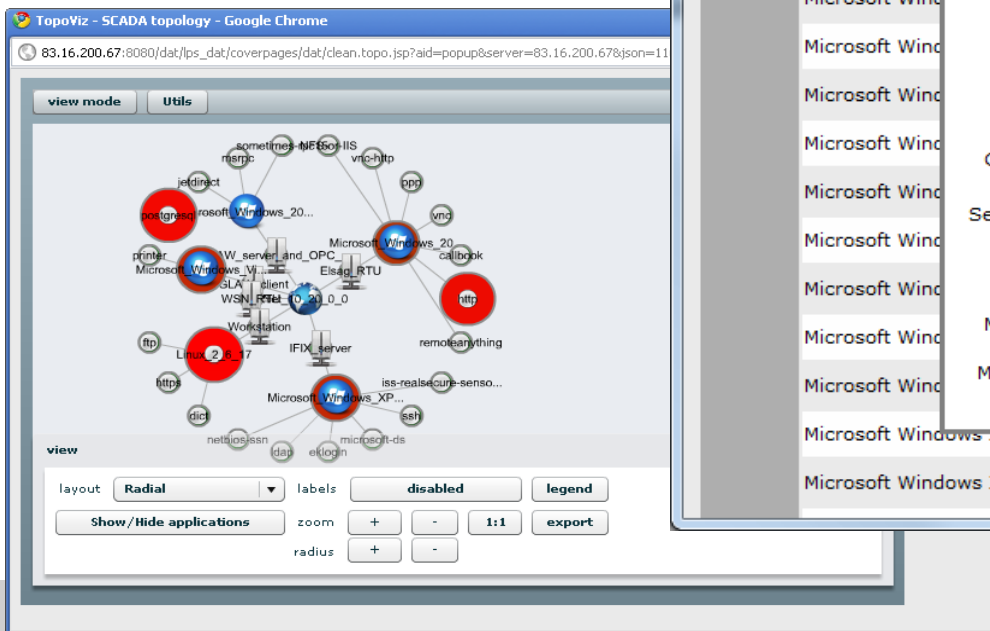
# Security audit



## 1. Topology visualization



## 2. Threat visualization



## 3. Security report

Welcome to Decision Aid Tool - Google Chrome

83.16.200.67:8080/dat/lps\_dat/coverpages/dat/checksystem.jsp?aid=popup

Język strony: angielski Chcesz ją przetłumaczyć? Tłumacz Nie Nigdy nie tłumacz z języka angielskiego

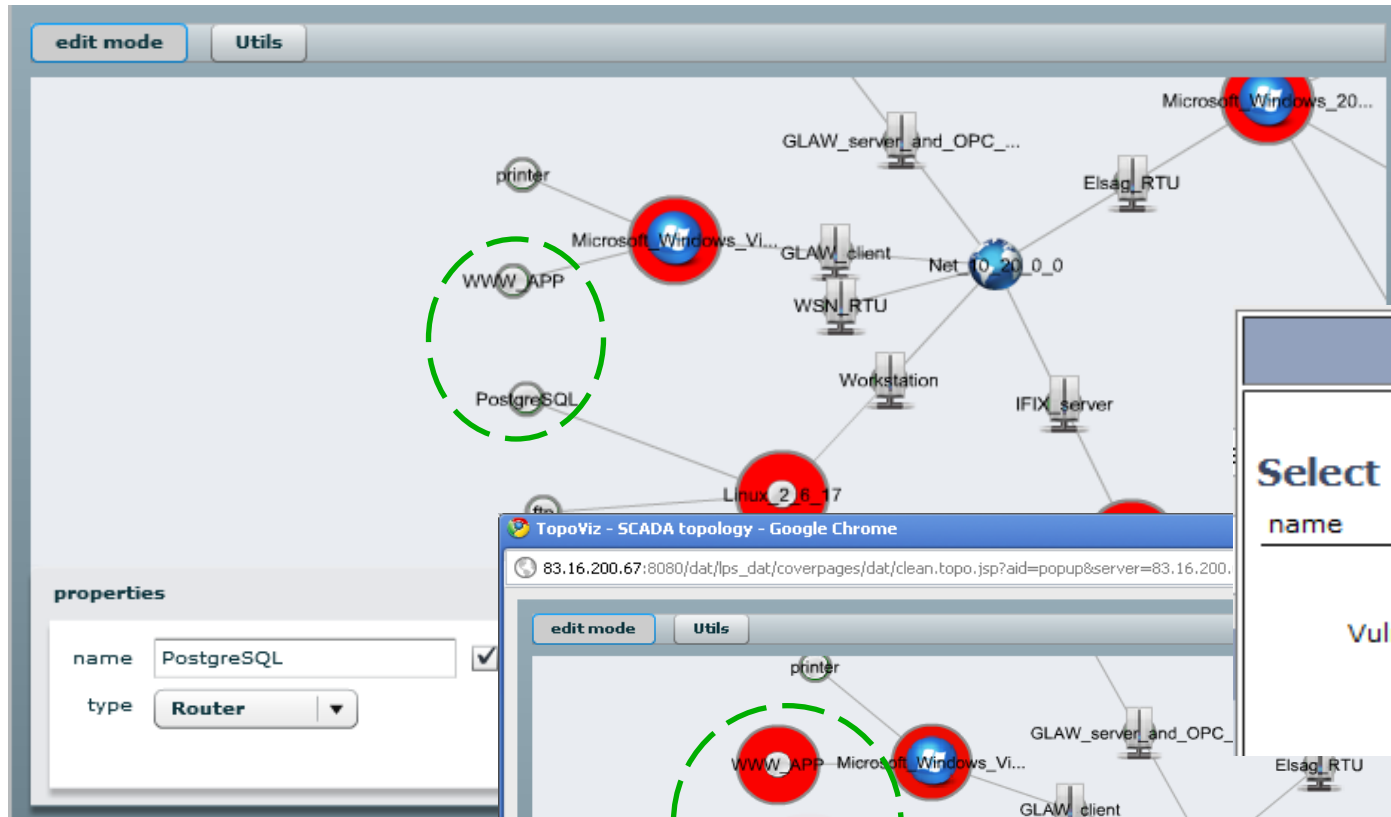
Rank	Asset	Threat	Severity level	Details
	Microsoft Windows Vista SP0	CAPEC-114	89.597	show
	Microsoft Windows Vista SP0	CAPEC-94	89.597	show
	Microsoft Windows Vista SP0	CAPEC-57	89.597	show
	Microsoft Windows Vista SP0	CAPEC-45	89.597	show
	Microsoft Windows XP SP2 or SP3	CAPEC-46	89.597	show

AT: Windows  
AS: F  
VSL: high  
CVE: The DNS client in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, and Vista uses predictable DNS transaction IDs, which allows remote attackers to spoof DNS responses.  
Description:  
CVSS Score: 8.8  
Asset: Microsoft Windows Vista SP0  
Severity level: 89.597  
Solution: CWE-287  
Threat: CAPEC-94  
Exploits: CVE-2008-0087  
Mitigation(s): -Architecture and Design - [Use an authentication framework or library such as the OWASP ESAPI Authentication feature.]  
Motivation(s): -Data Modification  
-Privilege Escalation  
-Information Leakage

# Simulation mode



1. These applications depend on each other

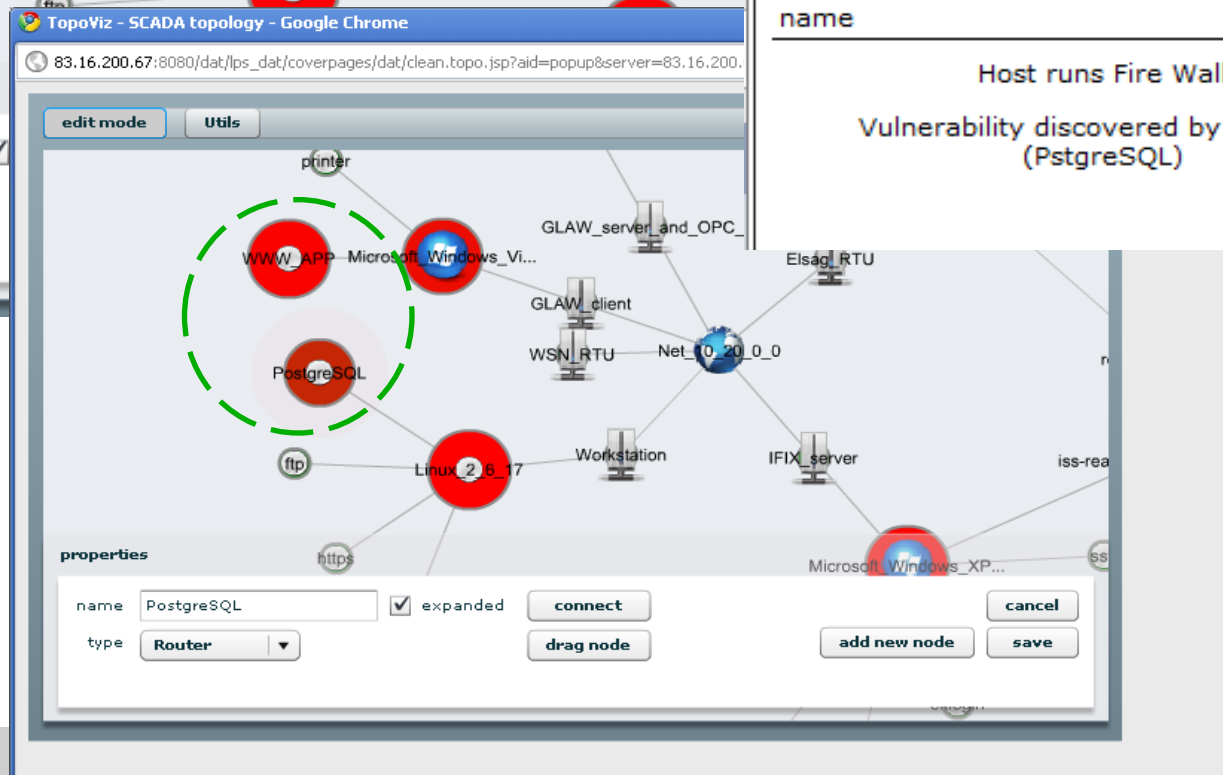


2. Injecting new vulnerability

close

Select set of facts:

name	action	enabled
Host runs Fire Wall	<a href="#">open</a>	<input type="checkbox"/>
Vulnerability discovered by operator (PstgreSQL)	<a href="#">open</a>	<input checked="" type="checkbox"/>



3. Result

# Security report



Welcome to Decision Aid Tool - Google Chrome

83.16.200.67:8080/dat/lps\_dat/coverpages/dat/checksystem.jsp?aid=popup

	Linux 2 6 17	CAPEC-52	83.001	<a href="#">show</a>
	Linux 2 6 17	CAPEC-85	83.001	<a href="#">show</a>
	Linux 2 6 17	CAPEC-28	83.001	<a href="#">show</a>
	Linux 2 6 17	CAPEC-171	83.001	<a href="#">show</a>
	Linux 2 6 17	CAPEC-91	83.001	<a href="#">show</a>
	Linux 2 6 17	CAPEC-281	83.001	<a href="#">show</a>
	Linux 2 6 17	CAPEC-59	83.001	<a href="#">show</a>
	Linux 2 6 17	CAPEC-60	83.001	<a href="#">show</a>
5	postgresql	CAPEC-35	79.761	<a href="#">show</a>
	postgresql	CAPEC-77	79.761	<a href="#">show</a>
	http	CAPEC-22	79.761	<a href="#">show</a>
	http	CAPEC-114	79.761	<a href="#">show</a>
	http	CAPEC-94	79.761	<a href="#">show</a>
6	PostgreSQL	PostgreSQL T	79.681	<a href="#">show</a>
	WWW APP	Service integrity lost	79.681	<a href="#">show</a>

# Business value modification



## 1. Applying new weights

Bayesian Network Properties:  
changes saved...

Vulnerability Severity Importance:

High

Medium

Low

Asset type bussines value:

WIN OS

Linux OS

SW  ←

HW

Safeguard Importance:  
If applied

save

## 2. Old report

	Linux 2 6 17	CAPEC-28	83.001	show
	Linux 2 6 17	CAPEC-171	83.001	show
	Linux 2 6 17	CAPEC-91	83.001	show
	Linux 2 6 17	CAPEC-281	83.001	show
	Linux 2 6 17	CAPEC-59	83.001	show
	Linux 2 6 17	CAPEC-60	83.001	show
	postgresql	CAPEC-35	79.761	show
	postgresql	CAPEC-77	79.761	show
5	http	CAPEC-22	79.761	show
	http	CAPEC-114	79.761	show
	http	CAPEC-94	79.761	show
	http	CAPEC-57	79.761	show
6	PostgreSQL	PostgreSQL T	79.681	show

## 3. New report

	Linux 2 6 17	CAPEC-91	83.001	show
	Linux 2 6 17	CAPEC-281	83.001	show
	Linux 2 6 17	CAPEC-59	83.001	show
	Linux 2 6 17	CAPEC-60	83.001	show

# Conclusions



- **DAT supports SCADA operator (human in the loop) by visualizing threats and proposing safeguards**
- **Ontology-based approach allows operator to use DAT for different critical infrastructures (by replacing the ontology)**
- **DAT allows operator estimate the impact of particular action prior the physical modifications (estimating risk via simulation)**
- **Expert knowledge can be adapted with the ontology via the security rules**

# Selected References



- 1. Kozik R., Choraś M., Hołubowicz W., Fusion of Bayesian and Ontology Approach Applied to Decision Support System for Critical Infrastructures Protection, In J. Alonso-Zarate and O. Hoffmann (Eds.): Mobile Lightweight Wireless Systems, LNICST 45, pp. 451–463, 2010.**
- 2. Choraś M., Kozik R., Flizikowski A., Hołubowicz W., Ontology Applied in Decision Support System for Critical Infrastructures Protection, In N. Garcia-Pedrajas et al. (Eds.): Trends in Applied Intelligent Systems, IEA/AIE 2010, Part I, LNAI 6096, pp. 671-680, 2010.**
- 3. Choraś M., Flizikowski A., Kozik R., Hołubowicz W., Decision Aid Tool and Ontology-Based Reasoning for Critical Infrastructure Vulnerabilities and Threats Analysis, E. Rome and R. Bloomfield (Eds.): Critical Information Infrastructures Security, CRITIS 2009, LNCS 6027, pp. 98–110, 2010.**
- 4. Choraś M., Stachowicz A., Kozik R., Flizikowski A., Renk R., Ontology-based approach to SCADA systems vulnerabilities representation for CIP, Electronics, vol. 11/2009, 35-38, November 2009.**