



FP7 Proposal discussion for Call 1

IST 2006 Helsinki
SecurIST Networking session
Nov 22nd 2006



Virtualisation, modelling and simulation to contextualise learning for attack mitigation and alerts management

atta.badii@rdg.ac.uk

- The prize is maintaining practical, affordable, resilient security protection pathways for the organisation
- Need to provide enterprise-wide Solutions Systems not just optimised algorithms (BF&I)
- New security solution integration pathways can size-able to perceived risk mitigation needs
- Sub-systems for organisational risk assessment calibration and learning



Needs

Need Continuous Learning and Knowledge Integration capability at various levels:

1. Real-time inline attacks detection and neutralising
2. Offline Attack Mitigation
3. Alerts and Vulnerabilities Prioritisation & Reporting
4. Overall Security Policy and Management
5. Security RoI Transparency & Assurance
6. Security Function Re-engineering for higher efficacy and RoI (Policy & Enactment)

Consortium Chemistry

- 1) Research Organisations with expertise in
 - Mathematical Modelling & Simulation
 - Pattern Recognition and Parallel Processing
 - Telecommunication Protocols
 - Security Attack Mitigation (IPS/IDS etc)
 - Embedded Systems
- 2) Industrial Partners as solution providers and integrators in IPS with Real Attacks Data, Embedded Systems Engineering
- 3) Industrial Partners as Users willing to provide real test environments

Contact atta.badii@rdg.ac.uk