PANOPTESEC

Dynamic Risk Management for Cyber Defence

PANOPTESEC is producing a cyber defence decision support system that will account for the dynamic nature of information and communications technologies, and the always evolving capabilities of cyber threats.

Innovating the Cyber Defence Technology

1 AUTOMATION OF ATTACK AWARENESS AND RISK ASSESSMENT

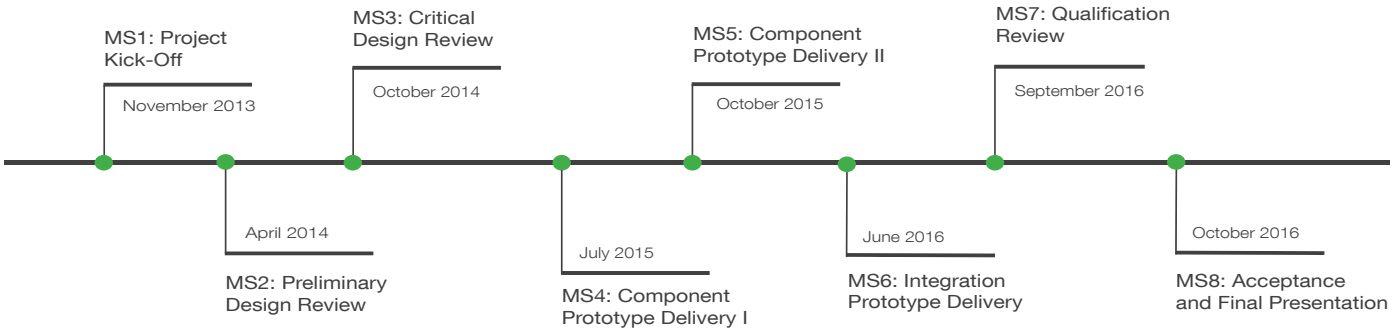
- **ATTACK MODELLING**
  Includes dynamic aspects of systems, services, threats, system vulnerability, and mission priority
- **AUTOMATED RISK QUANTIFICATION**
  based on attack graph models and mission dependency
- **SEPARATION OF RISK EVALUATION**
  into proactive and reactive treatment chains

2 ADVANCED MECHANISMS
to capture and model mission and business process relationships to service and system dependencies

3 SUPERIOR VISUALIZATION TECHNIQUES
for mission and business process risk display. Includes the representation of risk levels derived from risks in supporting services and systems

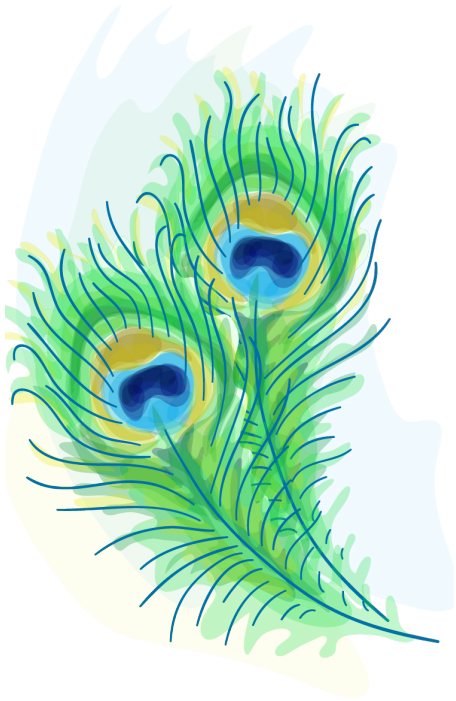
4 RESPONSE ASSISTANCE AUTOMATION
to provide cyber defence operators with prioritised courses of action, recommendation for review and activation

Milestones of the PANOPTESEC Consortium



PANOPTESEC Consortium

RHEA GROUP · SAPIENZA UNIVERSITÀ DI ROMA · acea · UNIVERSITÄT ZU LÜBECK INSTITUT FÜR INFORMATIONSSYSTEME · epistematica · TELECOM SudParis · NOKIA · Supélec



A Cyber Security System for Business and Operations

The PANOTESEC initative has led to the creation of two product lines: Business Risk Management and Security Incident Management. These cover a full range of security services at both business and operational levels. The decision support system operates according to integrated proactive and reactive treatment chains, protecting organizations from cyber security breaches.

The Elements Behind the Security Portfolio

Automated collection and correlation of system configuration, status, and events from multiple sources.

Automated collection and correlation of cyber security system data (e.g., vulnerability scanner data, intrusion detection system data) from multiple sources.

Accurate identification and capturing of the mission or business process dependencies on supporting networks and systems in a repeatable manner.

Automated assessment of mission and business process risks in response to the dynamic nature of the networks, systems, and threats.

Automated calculation of the priority systems to defend based on mission or business process priorities. Complete mapping of the supporting networks and systems.

Automated derivation of prioritized risk response activities (courses of action) including prioritization of proactive and reactive mitigation actions.

Automated deployment of policy based risk mitigation actions, following operator intervention.

For further information about the PANOPTESEC initiative, you are kindly invited to contact Douglas Wiemer, Member of the PANOPTESEC Steering Committee, at d.wiemer@rheagroup.com

Follow PANOPTESEC

www.panoptesec.eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 610416.