SIEM Systems of the Future

Roland Rieke / Fraunhofer SIT

Effectsplus Trustworthy ICT Research Roadmap Session
Cluster Meeting 29/30 March 2011

(1) Changes and developments

- **The Internet is driving a complete re-think of the paradigm whereby organizations deploy and manage their own services and infrastructure**
  - services get outsourced into clouds
  - infrastructures evolve hybrid - real & virtual
- **Cyber-physical Systems of Systems**
  - get connected to the Internet (IoT)
  - use meshed wireless communication structures

(2) Vision

- **Services & infrastructure in clouds**
  - leads to deployment of SIEM in clouds
  - scalable, inter-organizational, cross-level SIEM
- **New opportunities and risks**
  - inter-organizational analyses are possible
  - but raises issues on ensuring privacy and integrity of the events of any particular company
  - IoT enables new remote attacks against critical services & infrastructures
  - adaptive countermeasures
- **Entails different thinking about the revenue model**

(3) Challenges

- **Security, resilience, privacy**
  - security & privacy preservation for cloud applications & service infrastructures
  - intrusion tolerance, self-protection and self-healing
  - new cryptographic techniques enabling *processing of data in a privacy-preserving manner*
- **High-level situational security awareness**
  - provide cross-layer, cross-domain security information
  - *predictive analysis* of upcoming security problems
- **Adaptive response**
  - anticipatory impact analysis & decision support
  - technical but also legal challenges

(4) Solutions and implied RTD needs

- **Resilient, trust-enabling architecture**
  - *trusted collection* of security-relevant data from highly heterogeneous *trusted* networked devices (IoT)
  - resilient Internet-based backbone communication
- **Scalable security situation assessment**
  - scalable distribution of acquisition & parallel processing
  - seamless function splitting core engines/edge collectors
  - parallel data streaming to SIEM in clouds
  - multi-level, multi-domain security event processing
- **Cross-layer reasoning & mitigation**
  - adaptive configuration of policies & countermeasures

(6) The overview map from your project

Project name: MASSIF			
Developments and changes	**Future vision**	**Challenges and gaps**	**Future solutions and research needs**
services go cloud	SIEM go cloud	security, resilience, privacy	trust enabling architecture
virtual infrastructure	scalable, inter-organization SIEM	high-level situational security awareness	scalable security situation assessment
cyber-physical SoS go Internet	re-think revenue model	adaptive response	cross-layer reasoning & mitigation

Note to authors, this is summary that captures the previous points, the 'blobs' should contain keywords that correspond to the key points in your presentation.
Don't present this slide, we will use this to add to the combined roadmap that we will build in the session