Management of Security Information and Events in Future Internet

Who? Andrew Hutchison[1] Roland Rieke[2]

From? [1]T-Systems South Africa

[2]Fraunhofer Institute for Secure Information Technology SIT

When? **CS-GA 2011**

Overview

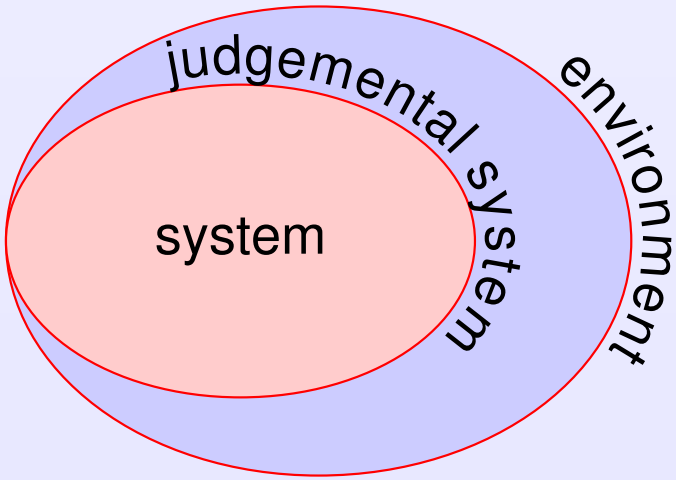
Changes and developments	Management of Security Information and Events (SIEM) in Future Internet (FI)
Vision	New opportunities & new risks
Challenges	Security, resilience, privacy
Solutions and implied RTD needs	Current and future research

Security Information and Event Management Systems

Product oriented view

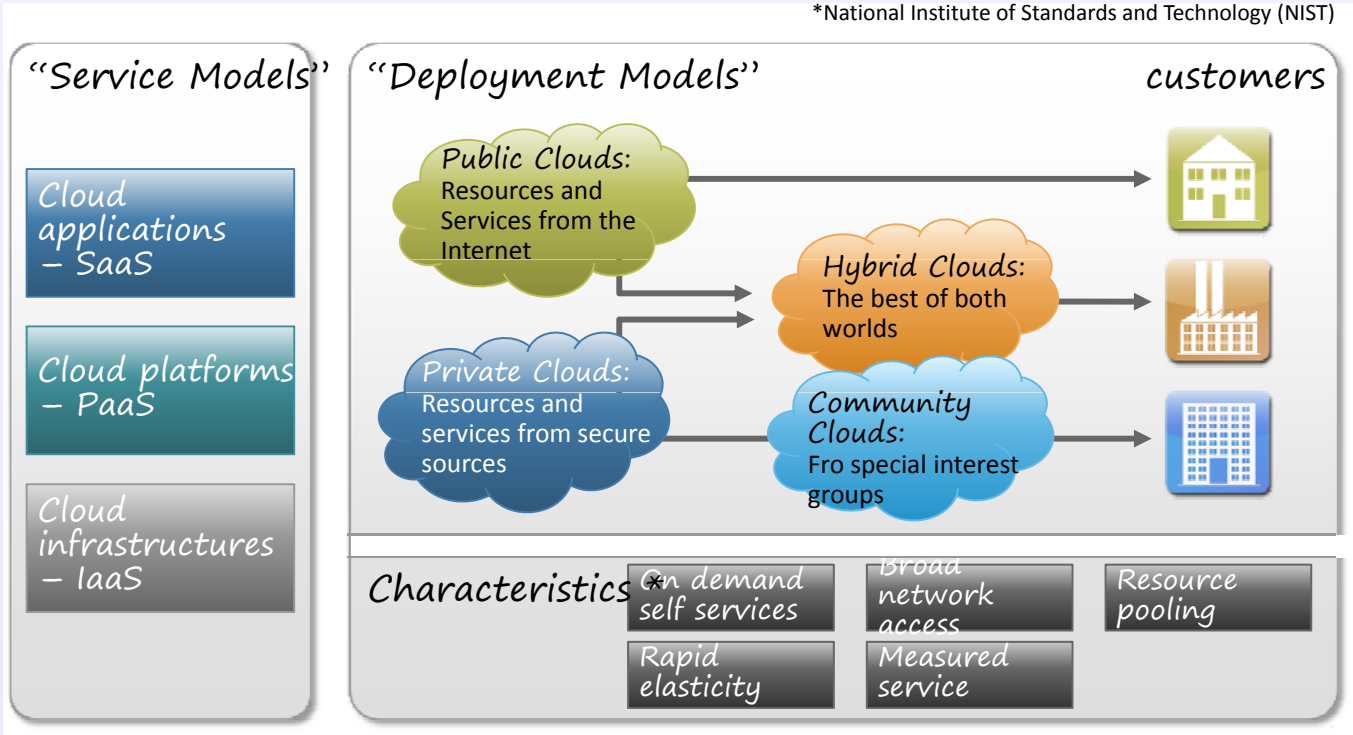
“SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes. ”
(Wikipedia, May 2011)

"Systems Come in Threes!
. . . a judgemental system, is involved in determining whether any particular activity (or inactivity) of a system in a given environment constitutes or would constitute - from its viewpoint - a failure."
(Brian Randell, IFIP WG 10.4, Guadeloupe, 2007)



Changes and developments

Future Internet (FI) is driving a complete re-think of the paradigm whereby organisations deploy and manage their own services and infrastructure



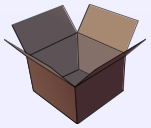
Source: T-Systems

- Services get outsourced into clouds
- Infrastructures evolve hybrid - real & virtual & spread across administrative domains and physical sites

Changes and developments

Cyber-physical Systems of Systems (SoS) get connected to the Internet

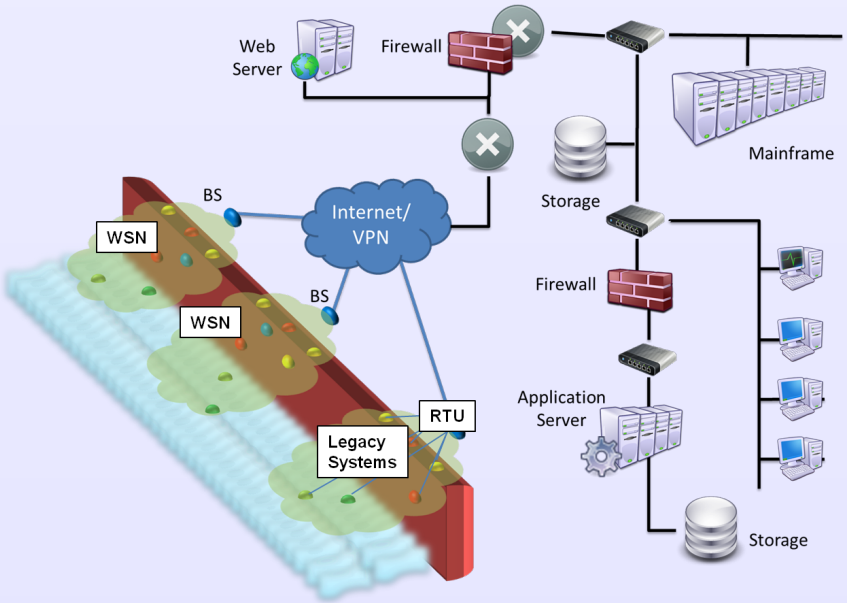
Smart Grid



IoT

Car-to-X

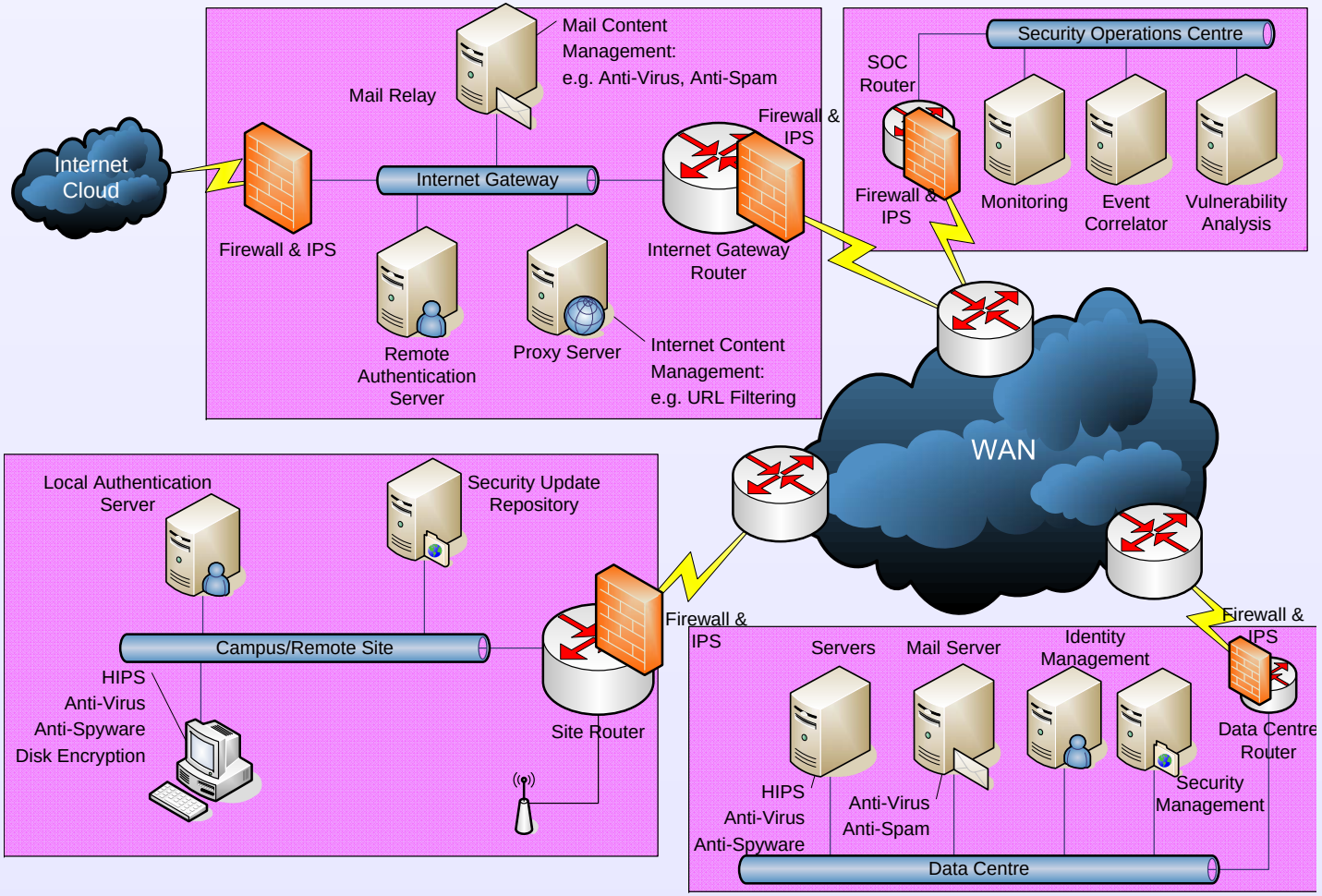
- Use of meshed wireless communication structures
- –> physical actuators get in reach of attackers



Source: MASSIF project (Epsilon)

Vision

Services & infrastructure in clouds leads to deployment of SIEM in clouds



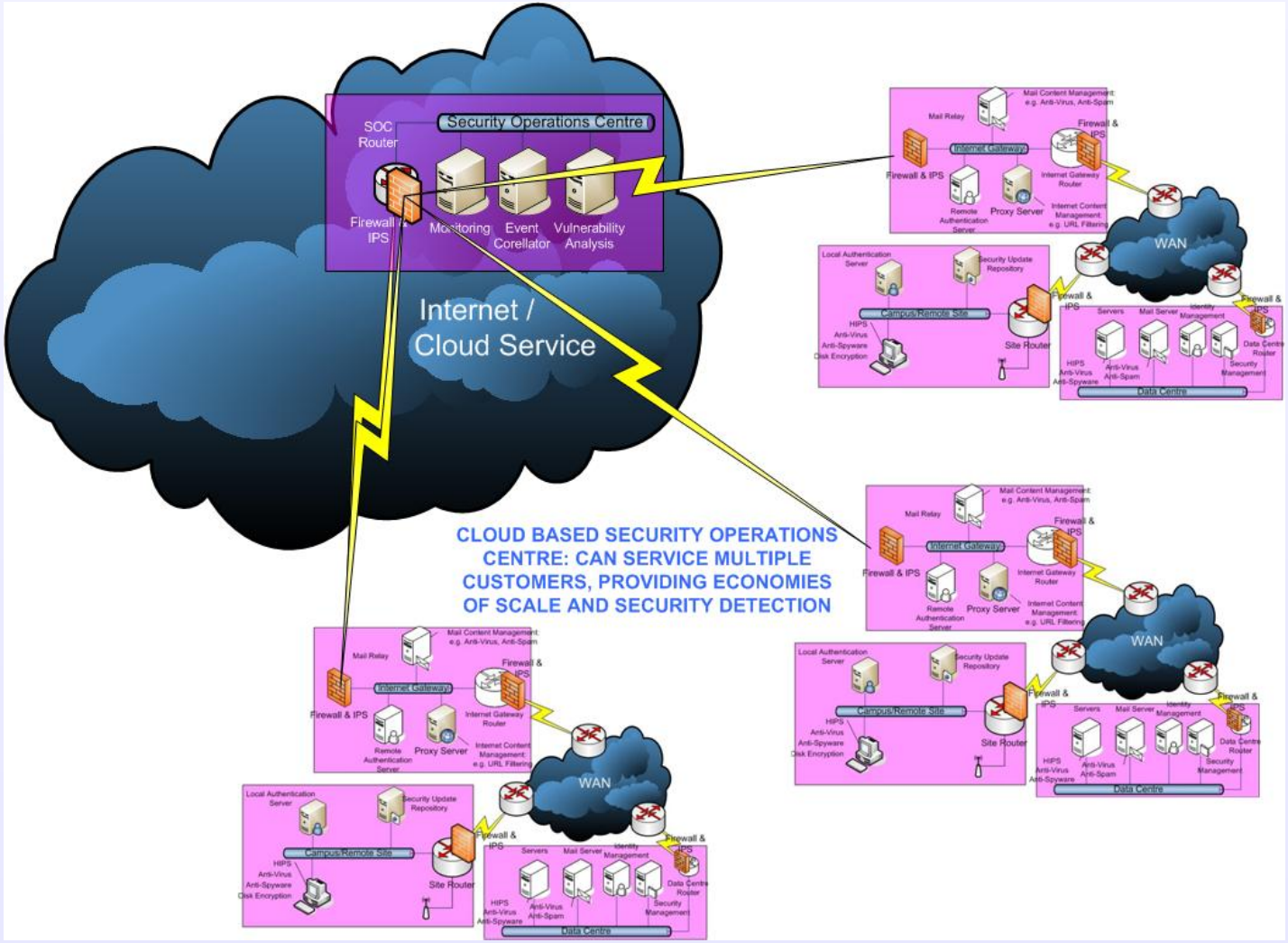
Source: T-Systems

Managed SIEM

Today, multiple sources are collected centrally within the realm of the provider organisation

Vision

Services & infrastructure in clouds leads to deployment of SIEM in clouds



Source: T-Systems

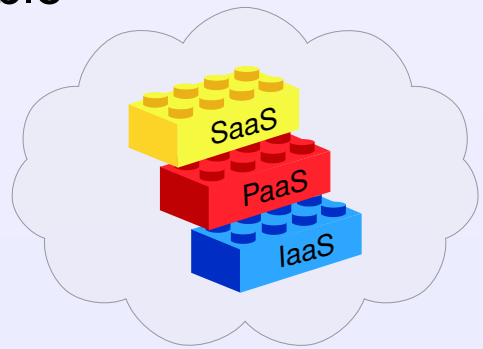
Future SIEM

Scalable, inter-organisational, cross-level

Vision

New opportunities

- Inter-organisational analyses are possible
- Adaptive countermeasures



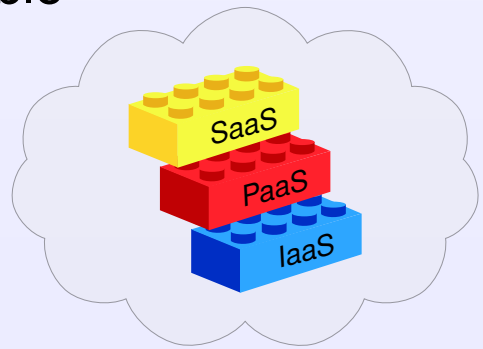
and new Risks

- Privacy and integrity of the events of any particular company
- Virtualisation layers introduce new vulnerabilities
- IoT enables new remote attacks against critical services & infrastructures

Vision

New opportunities

- Inter-organisational analyses are possible
- Adaptive countermeasures

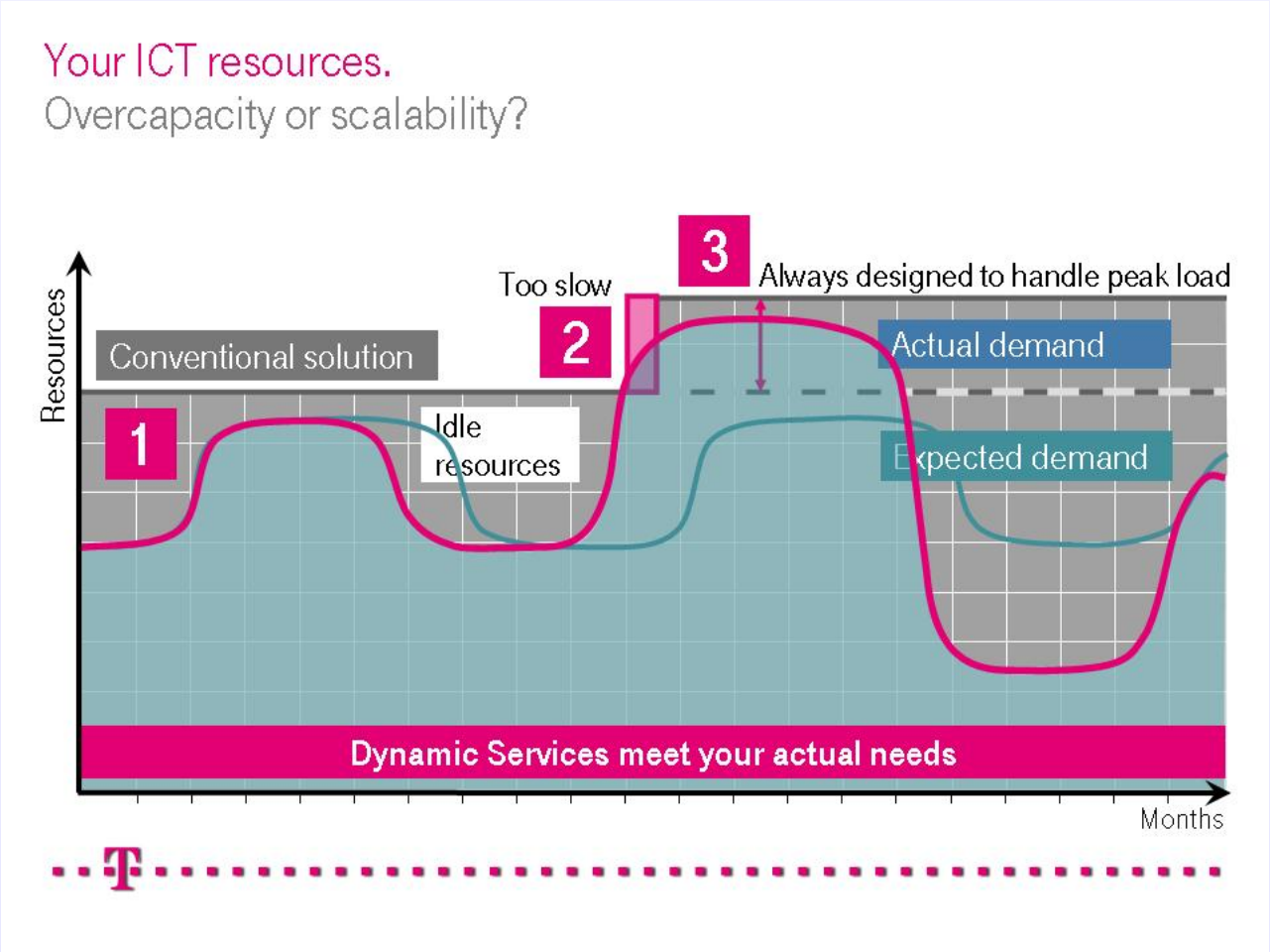


and new Risks

- Privacy and integrity of the events of any particular company
- Virtualisation layers introduce new vulnerabilities
- IoT enables new remote attacks against critical services & infrastructures

Vision

New SIEM deployment entails different thinking about the revenue model



Source: T-Systems

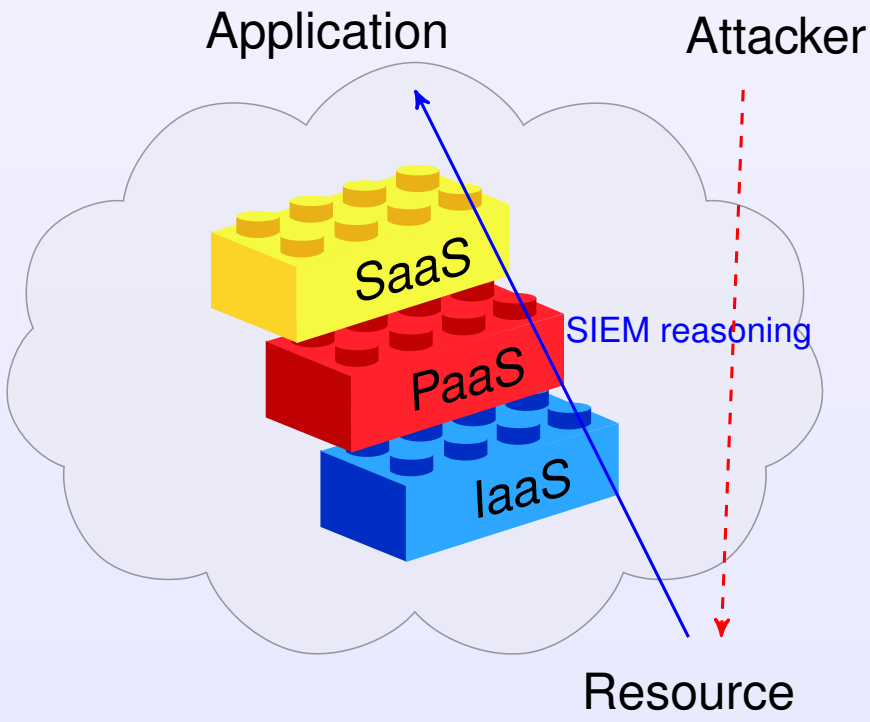
Challenges

Security, resilience, privacy

- Security for cloud applications & service infrastructures
- Intrusion tolerance, self-protection and self-healing
- QoS guarantees to *ensure reliable and timeous arrival of security event information* from the sensors
- The debate on *Internet net-neutrality* could also refer here since there could be a case for expediting *control traffic* such as SIEM event feeds
- New cryptographic techniques enabling processing of data in a privacy-preserving manner

Challenges

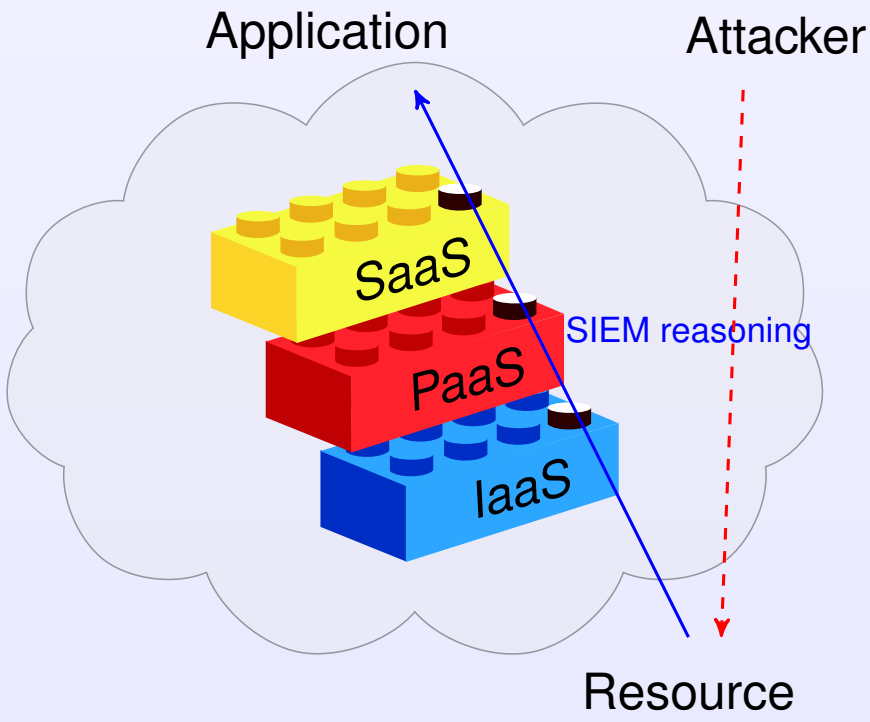
High-level situational security awareness



- Provide cross-layer, cross-domain security information
  ▷ given that the cloud hides technical delivery of the service from the SIEM provider (typically increasing for higher level services)
- SIEM needs limited transparency

Challenges

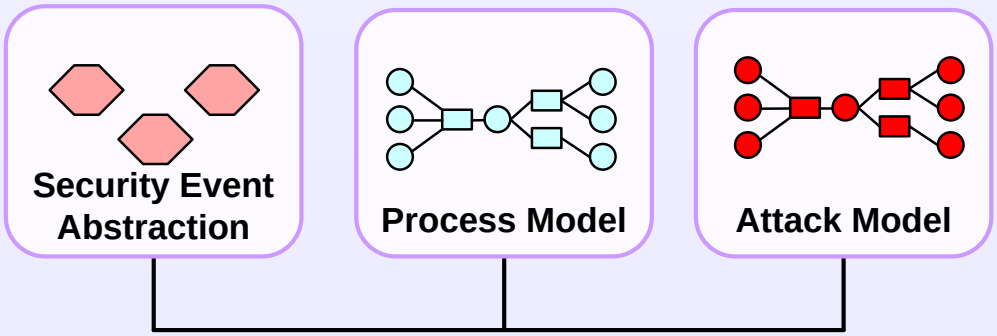
High-level situational security awareness



- Provide cross-layer, cross-domain security information
  ▷ given that the cloud hides technical delivery of the service from the SIEM provider (typically increasing for higher level services)
- SIEM needs limited transparency

Challenges

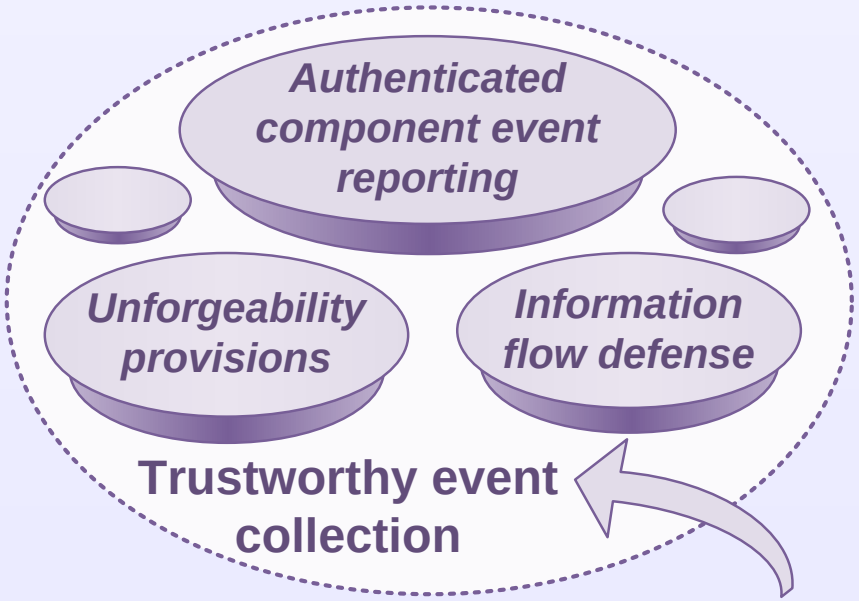
Adaptive response



- Predictive analysis of upcoming security problems
  ▷ given that customers have no insights on risk mitigation mechanisms of cloud providers and overall status
- Anticipatory impact analysis & decision support
- Technical but also legal challenges

Solutions and implied RTD needs

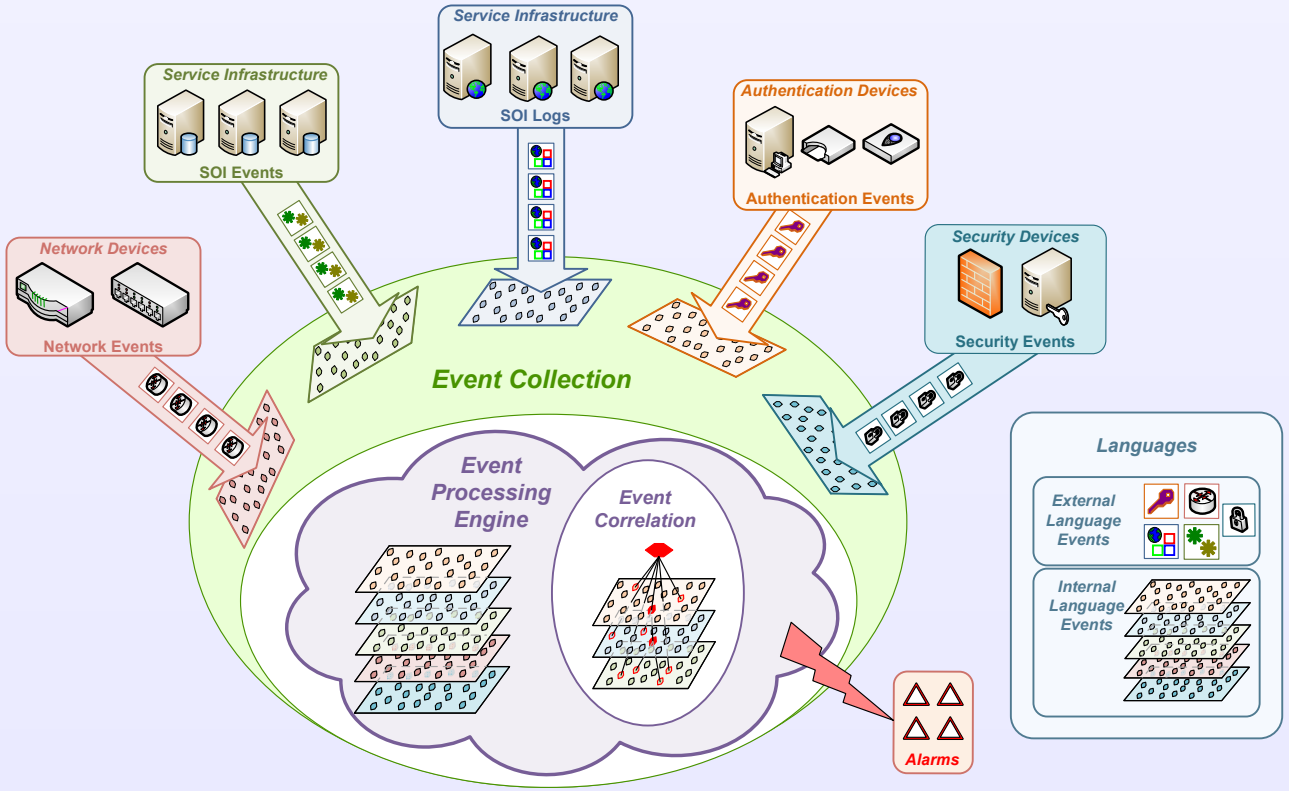
Resilient, trust-enabling SIEM architecture



- Trusted collection of security-relevant data from highly heterogeneous trusted networked devices (IoT)
- Resilient Internet-based backbone communication

Solutions and implied RTD needs

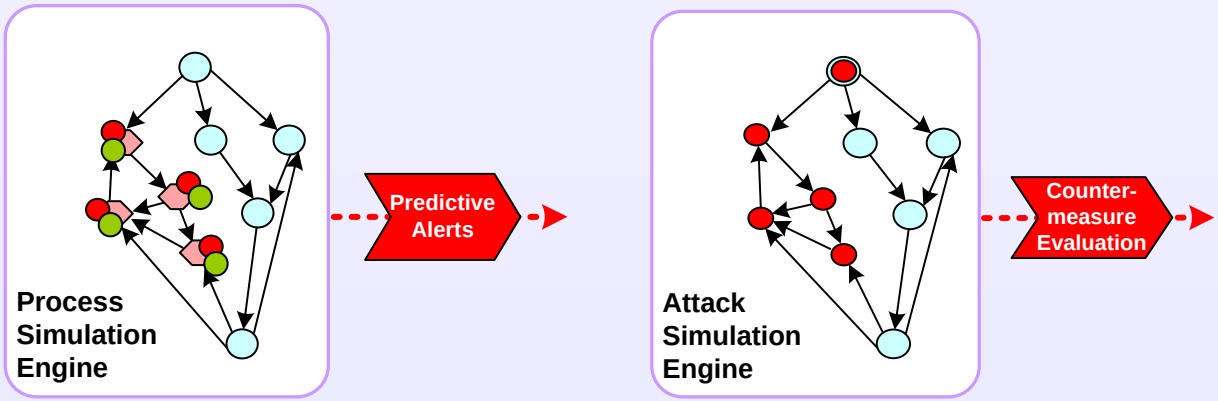
Scalable security situation assessment



- 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

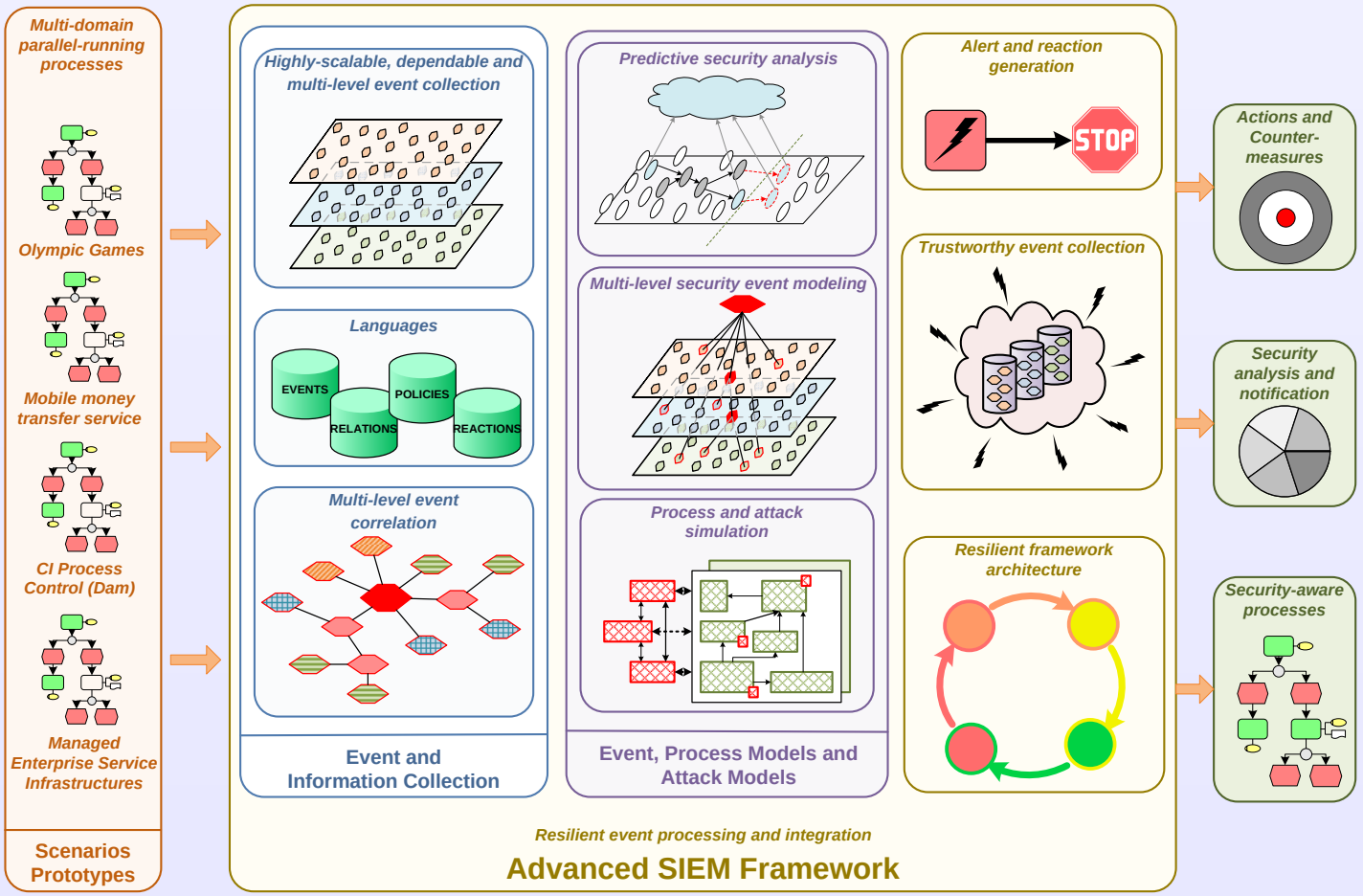
Solutions and implied RTD needs

Cross-layer reasoning & mitigation



- Multi-level security event modelling aims at a holistic solution to protect service infrastructures of FI
- Predictive security monitoring enables to fight attacks proactively by predicting their future actions
- Adaptive configuration of policies & countermeasures

A platform around which these thoughts are crystallizing!



www.massif-project.eu

Conclusions

Changes and developments

▷ FI is driving a complete re-think of the paradigm whereby organisations deploy and manage their own services and infrastructure

▷ Cyber-physical SoS get connected to the Internet

Vision

▷ Services & infrastructure in clouds leads to deployment of SIEM in clouds

▷ New opportunities and revenue models & new risks

Challenges

▷ Security, resilience, privacy

▷ High-level situational security awareness

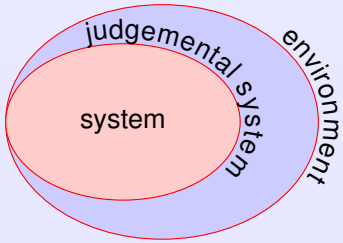
▷ Adaptive response

Solutions and implied RTD needs

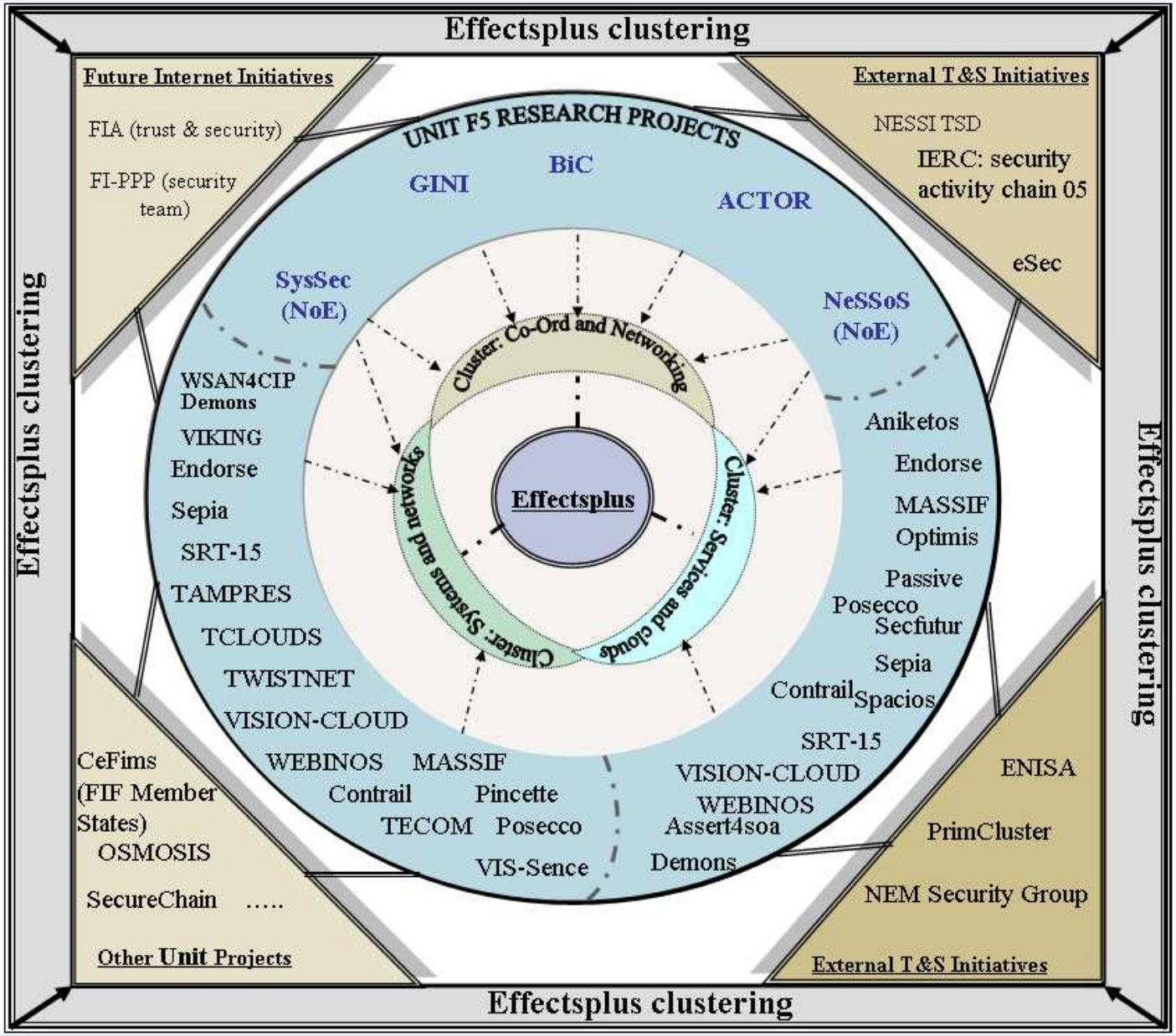
▷ Resilient, trust-enabling SIEM architecture

▷ Scalable security situation assessment

▷ Cross-layer reasoning & mitigation



Landscape of European Security Projects



Source: Frances Cleary (EFFECTS+ project)