Collaborative Security Model (CSM)

Security Architecture Vision 2015+

Christof Jungo

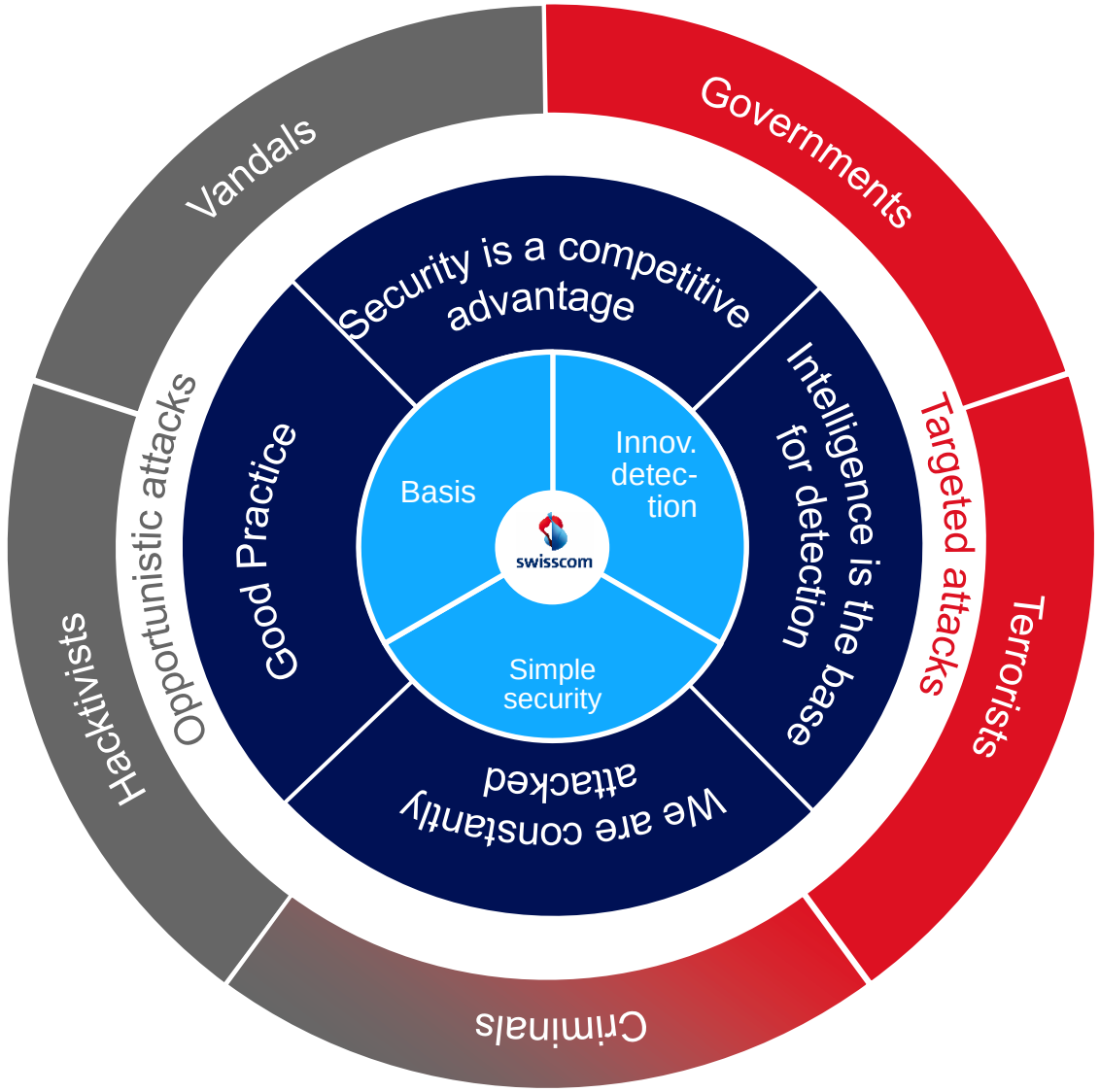
C2, internal use (SIGS)

23 June 2015

swisscom

Swisscom Security

Our Aspiration: «We build security for people in a connected world – always and everywhere»



swisscom

Various areas involved in the protection of the business

Targeted cooperation is required for success

Prevention	Detection	Intervention
> Proactive protection of data at various levels > Systems, Employees, Networks	> Early detection of attacks > Collection of information on intrusions from the Internet and the data	> Efficient and effective response to security incidents
> Training/awareness of employees (phishing campaign) > Continuity management > Resilience > Security risk management	> Data leakage prevention > Security information and event management (SIEM) > Threat intelligence > HoneyNet > Exchange with third parties	> Robust incident processes > Abuse and fraud management > Automated reactions > Disaster recovery and crisis management

Basic Principles

> Basic protection provisions, processes and technologies on which other measures are based

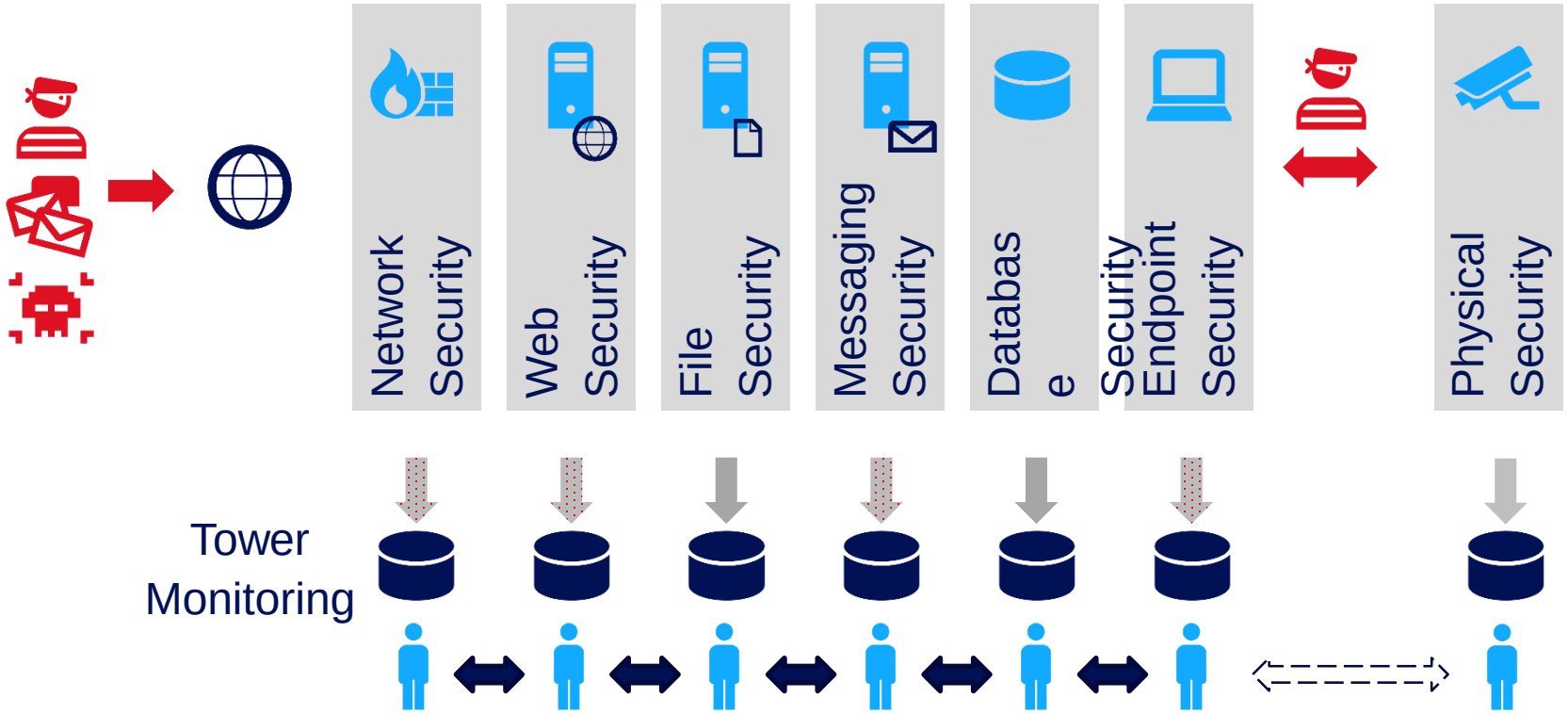
> Policy framework > Identity and access management > Physical security	> Cooperation with other organisations > Asset & risk inventory	> Knowledge about the threat situation > Firewalls, intrusion detection systems, antivirus software, …

Internal challenge

Environments have developed over time

Impact of IT Industrialisation

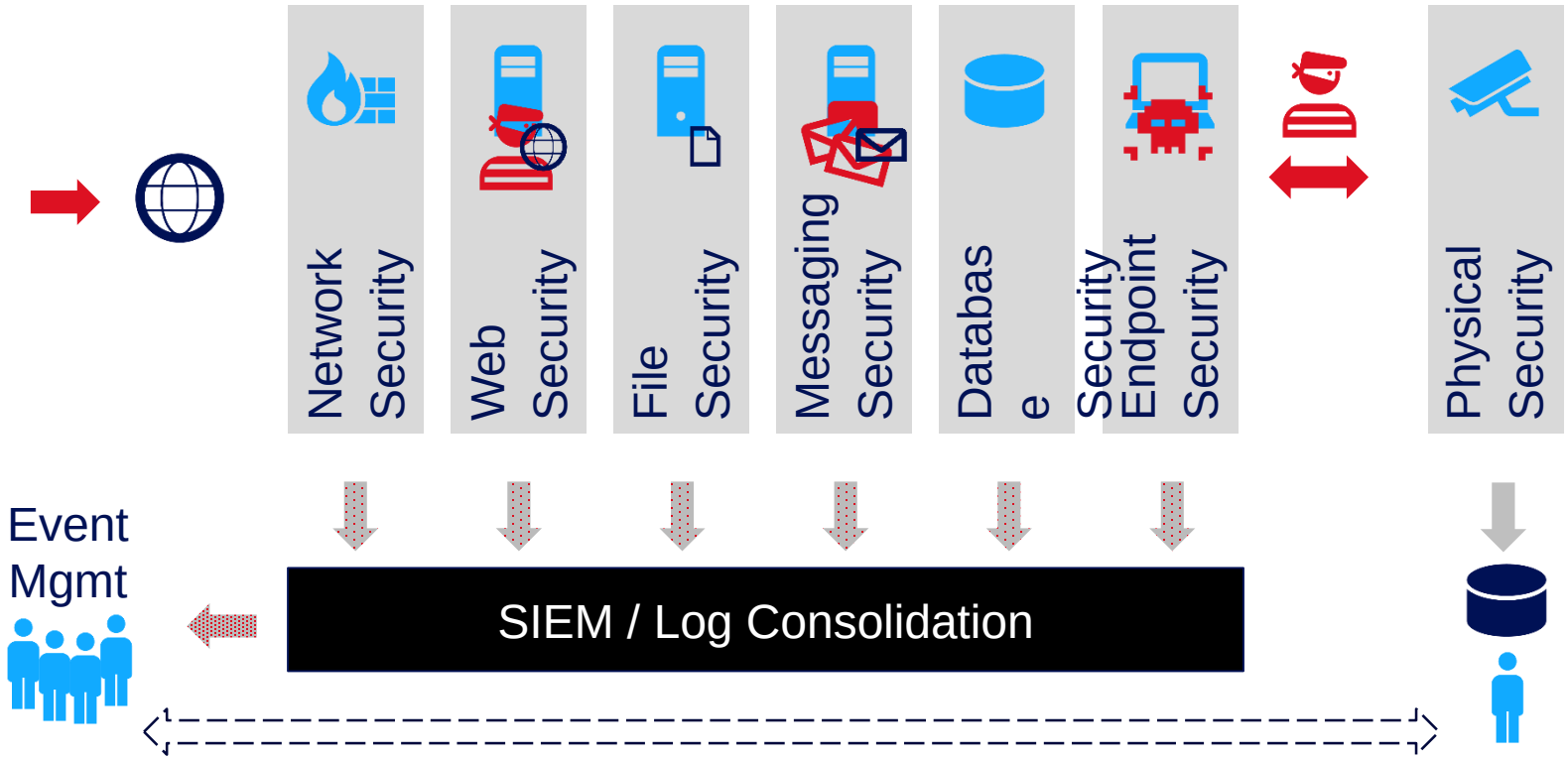
Silo landscapes and isolated analysis of security



Detection of security incidents: modest
Time requirement for coordination: high
Time requirement for remediation: high to very high
Integration costs: very high with umbrella systems

Centralisation and Consolidation

Increase in detection rate

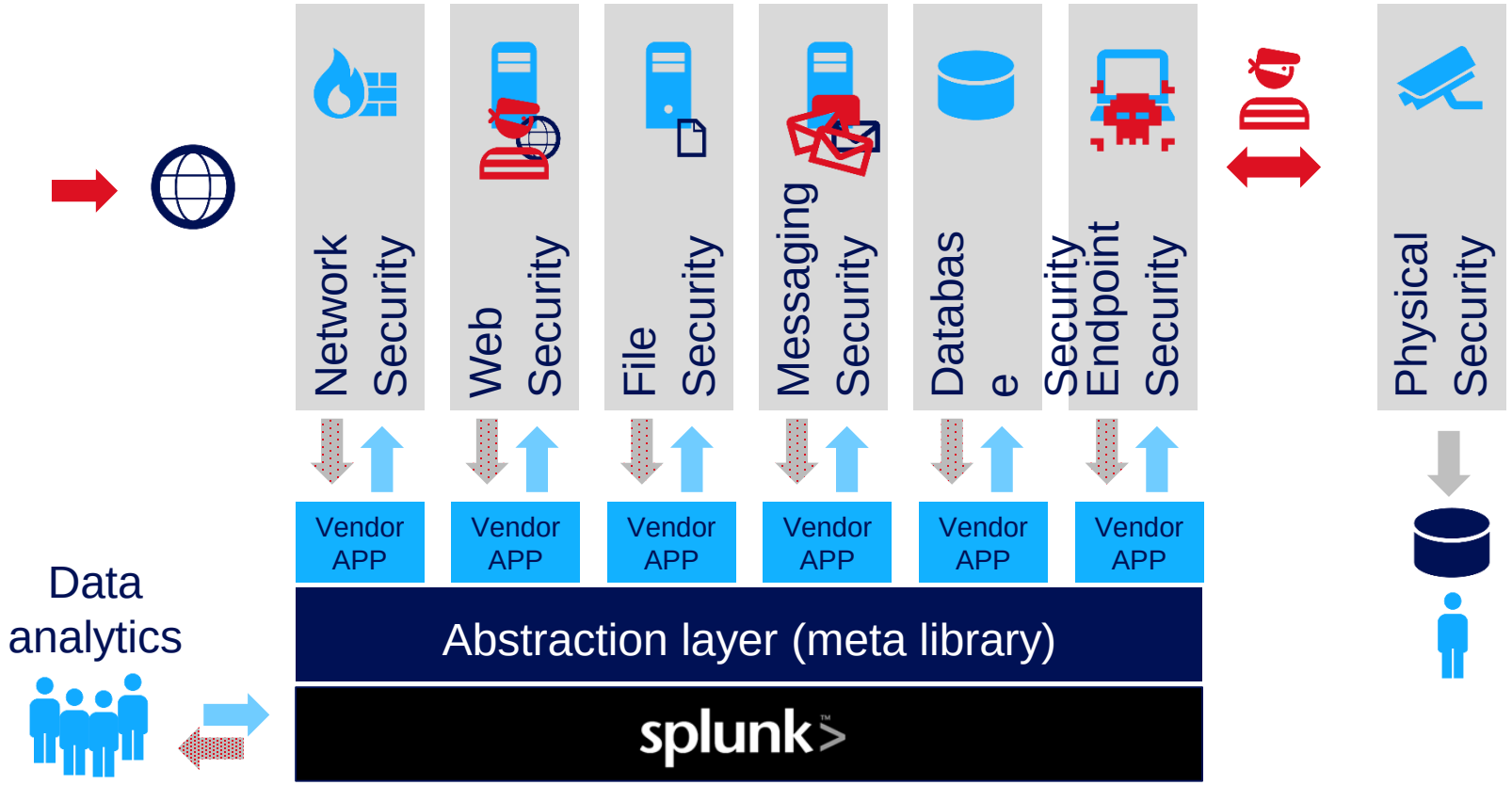


Detection of security incidents: good
Time requirement for coordination: average
Time requirement for remediation: average
Integration costs: high

swisscom

Active Response

Set-up of abstraction layer and response channel

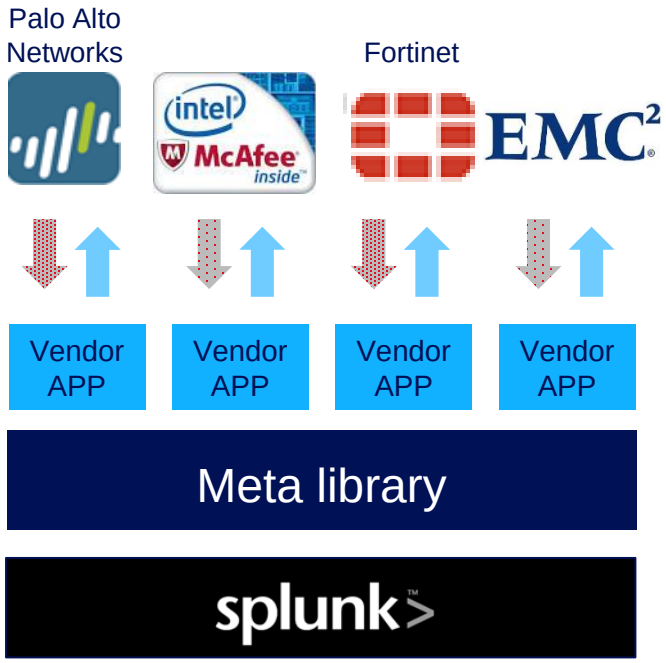


Detection of security incidents: good
Time requirement for coordination: low
Time requirement for remediation: low
Integration costs: low

swisscom

Prototype / demonstrator

Set-up of eco-system



Meta library

- Open and freely upgradeable abstraction layer for security commands as per CSS (design language in web design)
- Standardisation by a body aka W3C World Wide Web Consortium
- Integral element of Splunk (without additional costs)

Vendor APP

- Establishment of the communication channel
- Translation of the meta library into device-specific commands and configurations
- APP development by manufacturers
- APP store for manufacturers

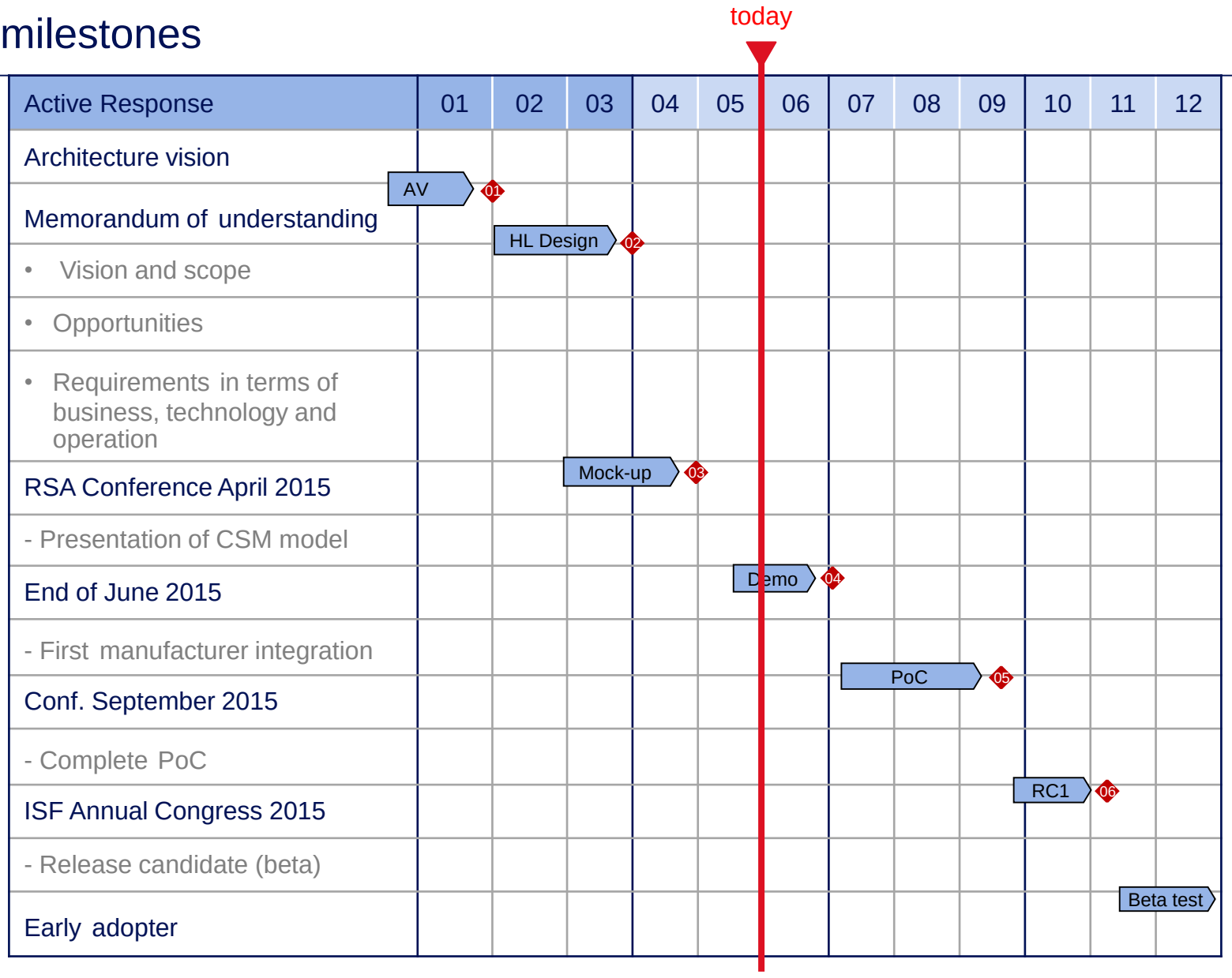
Onboarding

- Straightforward onboarding processes for manufacturers
- Quality assurance processes for APP

Collaboration and eco-system through open interfaces, easy integration and distributed development costs

The Path to Version 1.0

Planning and milestones



swisscom

Benefits of the Collaborative Security Model

Interaction and adaptability

The Collaborative Security Model

- reduces the dependence of security manufacturers and encourages them to improve the quality of their products
- enables interaction between various manufacturers
  - eco-system instead of silo landscape
- facilitates the integration of new components (Plug&Play)
- reduces management requirements (SoC & CSIRT) and costs

The market functions well if willingness to collaborate is part of the manufacturers' product strategy.

The focus is on simplicity, flexibility and dynamism

Upgrading the Eco-System

Support from the community

We can only achieve the greatest possible penetration together if

- You call upon your suppliers to take part in the eco-system (making APP available)
- Collaborative security model becomes part of the product requirements (demand management)
- The suppliers understand the benefits for them

We need your support in order to be successful

Only through collaboration and with an eco-system and a market that functions well will we achieve optimal security and be able to protect ourselves adequately.

swisscom