Trustworthy system operations

Artem Voronkov

PhD Student at KAU

artem.voronkov@kau.se

Agenda

- General overview
- Research objectives
- Workplan
- Event data collection and transfer

General overview

- To trust the system:
  - Security
  - Privacy
  - Reliability
  - Transparency

General overview

- Security plays an important role for trustworthy network services
  - Preventive measures (firewall, IPS, etc.)
  - Detective measures (IDS, SEM/SIEM, etc.)
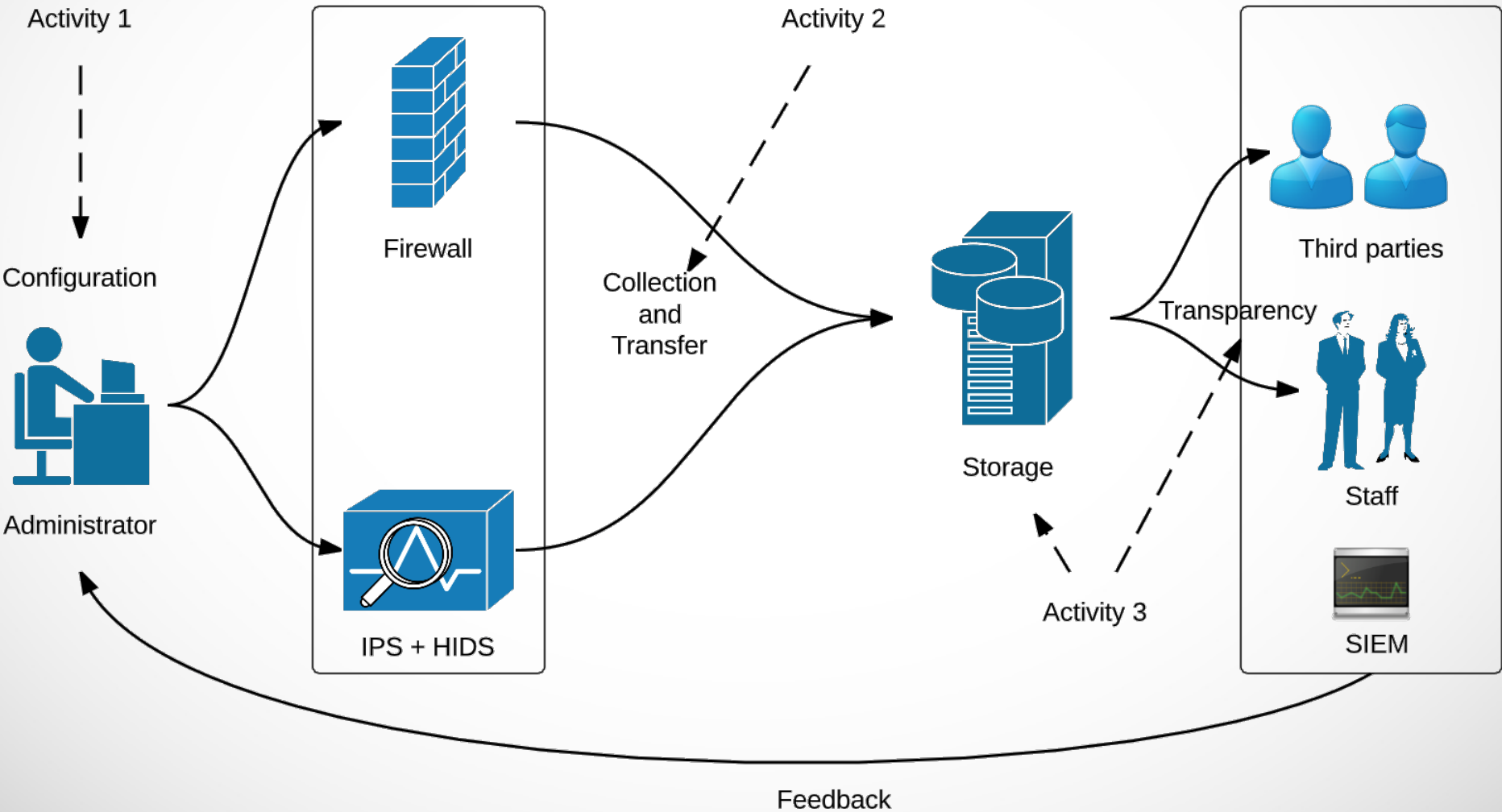- Event logging

General overview

Research objectives

- ## The overarching objective:

  Research efficient and usable security measures that lead to more trustworthy system operations for network services

- ## The key research issues:

  – Security control configuration

  – Efficient and secure event data collection and transfer

  – Secure event storage and transparency

Workplan

- Three parallel activities:
  - Security control configuration
  - Event data collection and transfer
  - Secure event storage and transparency

Event data collection and transfer

- Define realistic use cases
  - Goals for collecting event data
  - Involved entities
  - Some technical details
- Methodology
  - Performance evaluation of protocols
    - Simulations
    - Experiments

Thank you for your attention!