NETWORK DEFENCE USING ATTACKER-DEFENDER INTERACTION MODELLING

Wednesday 22nd June, 2016

Jana Medková
Pavel Čeleda

CSIRT-MU

Research Problem

Automated selection of response actions

Research Problem

Automated selection of response actions

- The cyber attacks grow both in **number** and **speed**

Research Problem

Automated selection of response actions

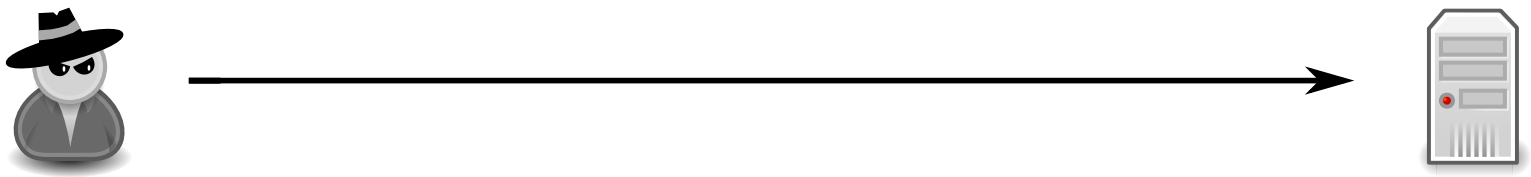
- The cyber attacks grow both in **number** and **speed**
- Network security still lacks an efficient attack response system capable of running autonomously

Research Problem

Automated selection of response actions

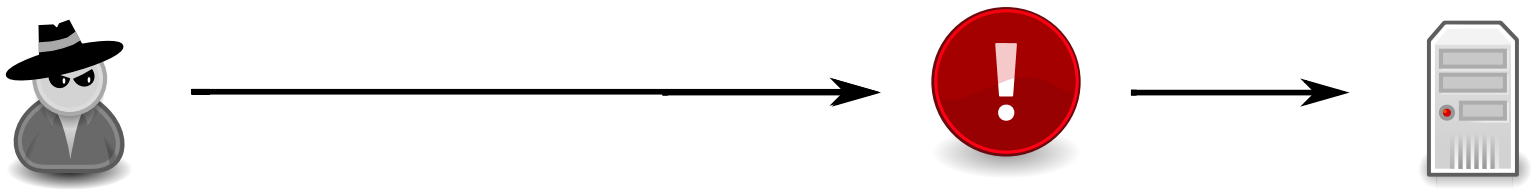
- The cyber attacks grow both in **number** and **speed**
- Network security still lacks an efficient attack response system capable of running autonomously
- Cyber attack and defence is very complex
  - We are always uncertain about the state of the network
  - We don’t know the attacker’s objectives and previous actions (and whether he is an attacker at all)
  - The number of attack vectors is ever growing

Attack Response

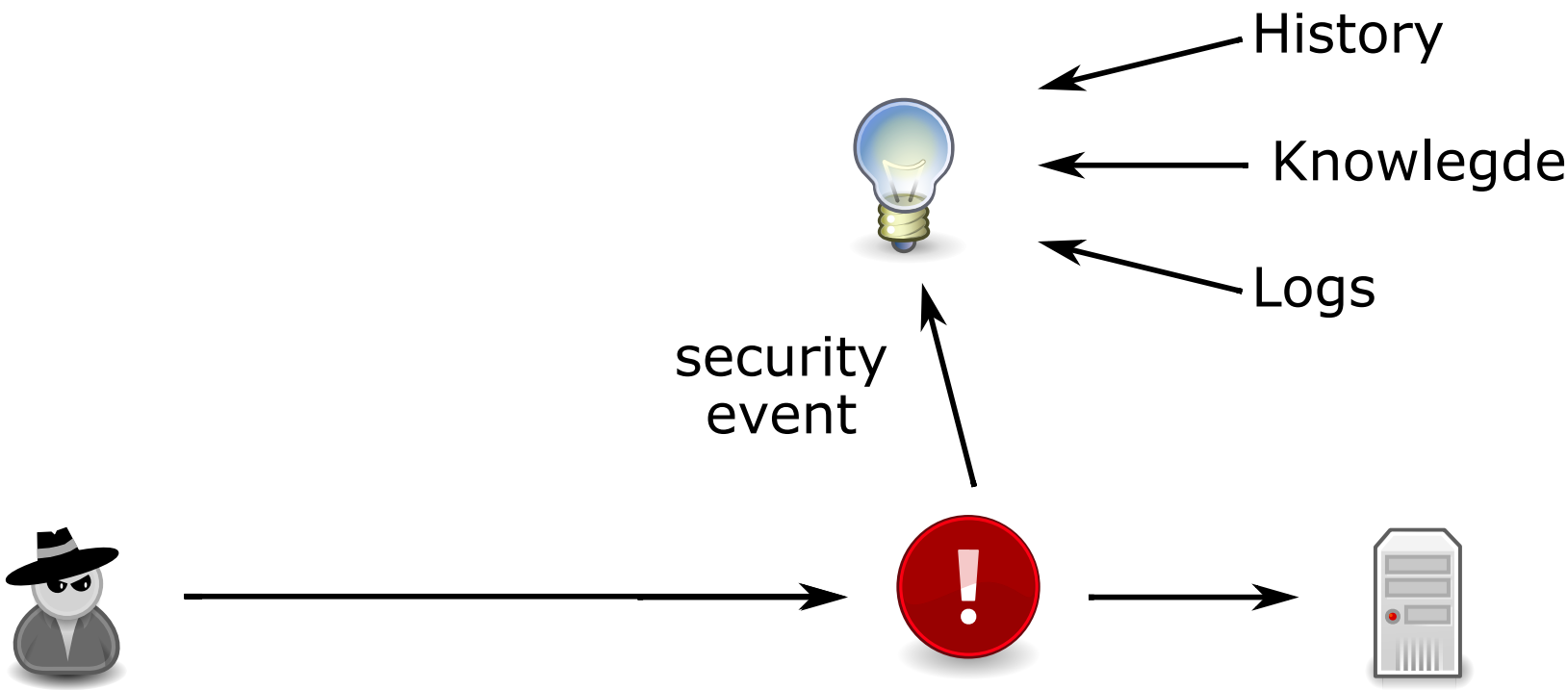


CSIRT-MU

Attack Response

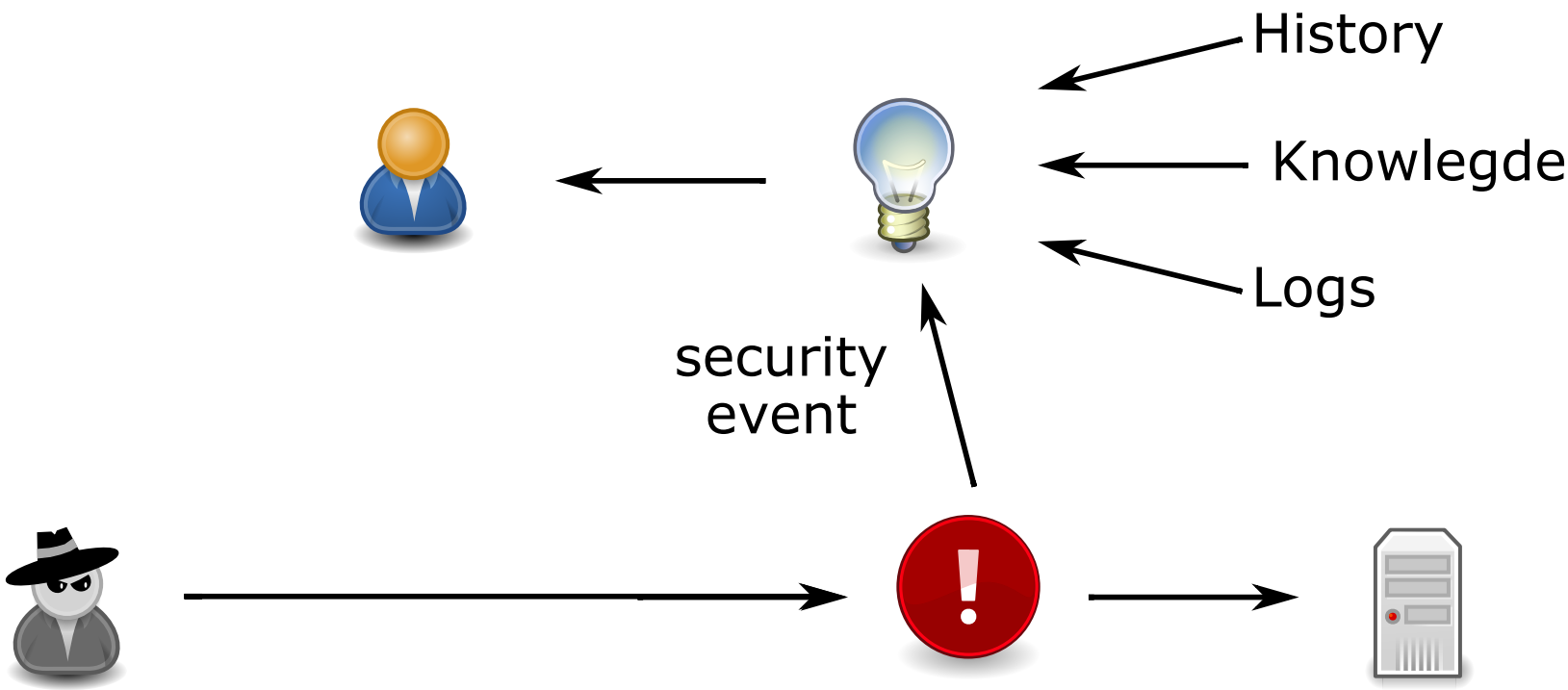


Attack Response



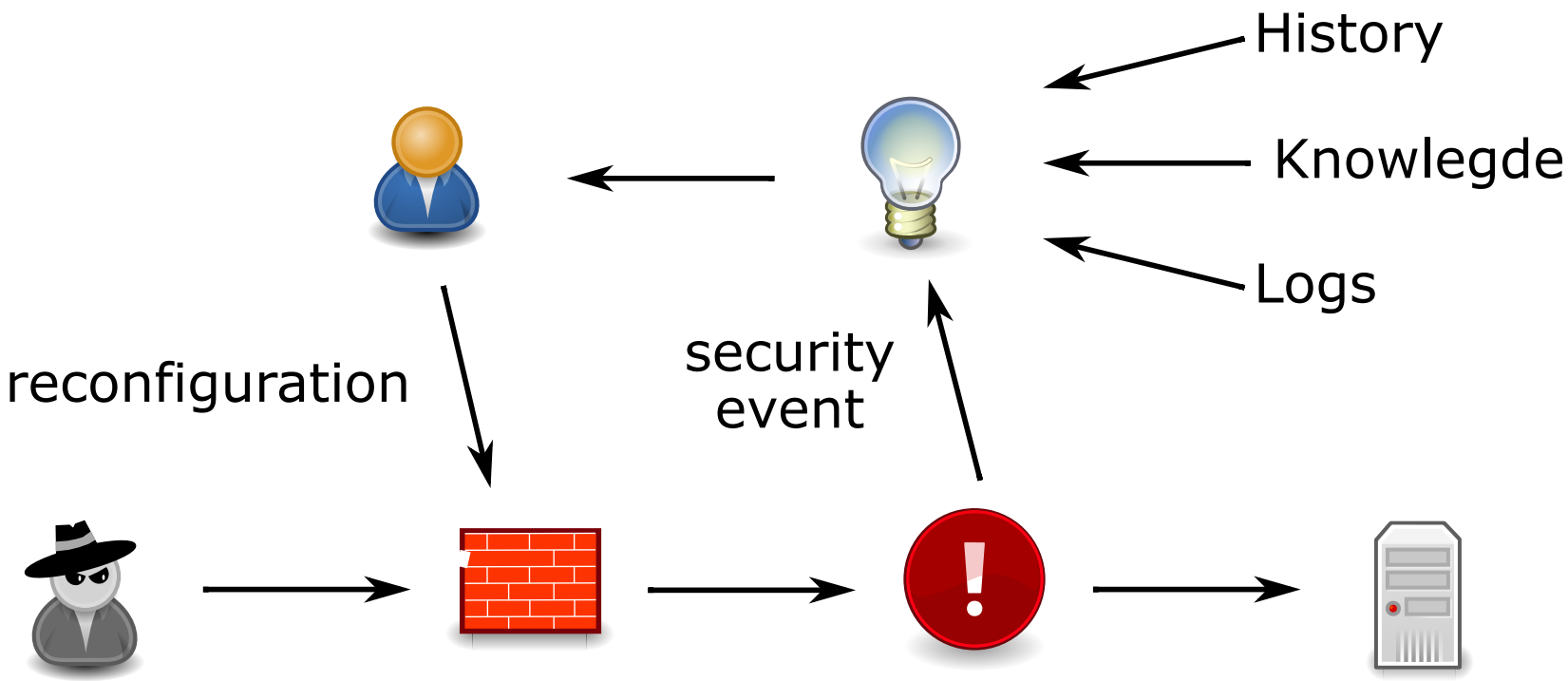
CSIRT-MU

Attack Response



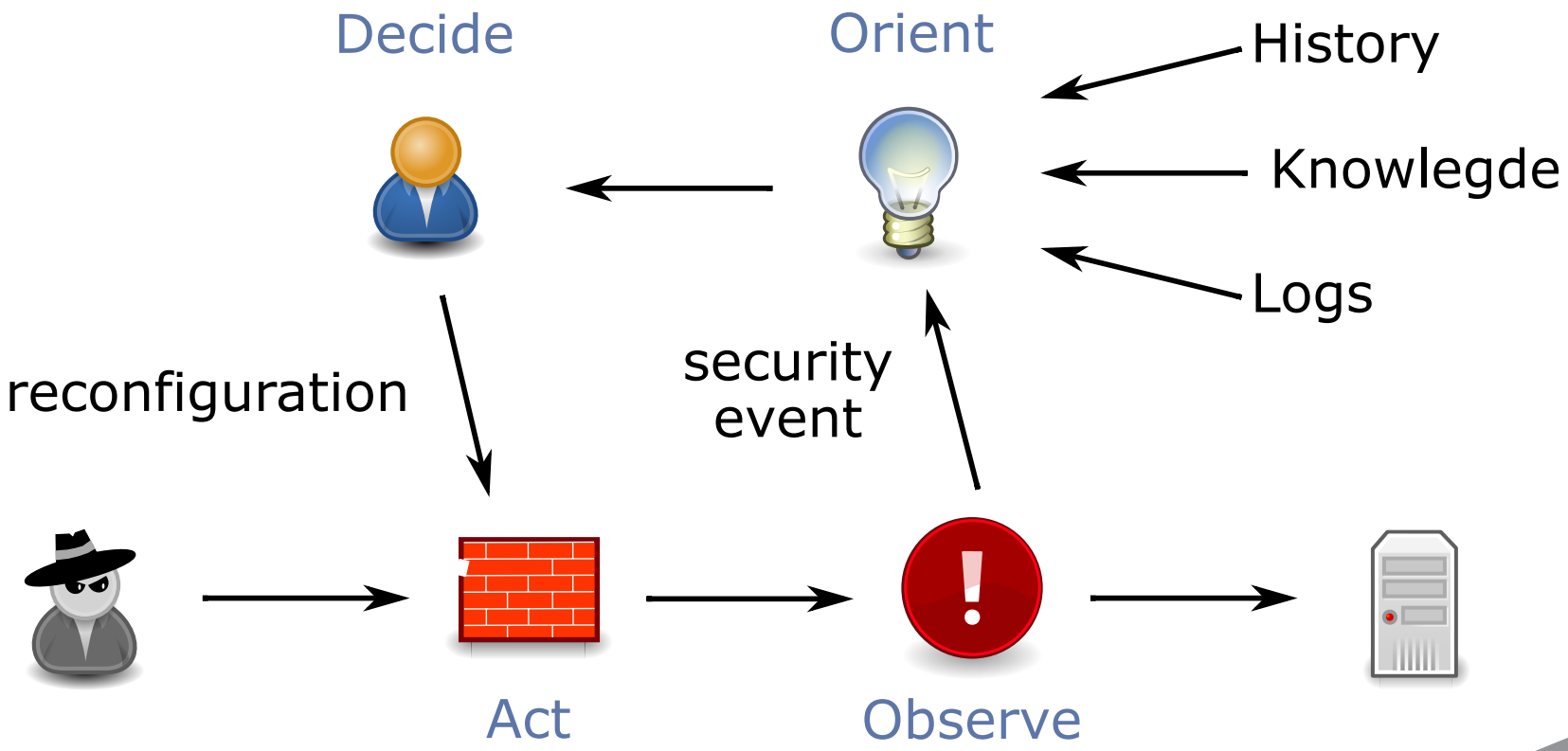
CSIRT-MU

Attack Response



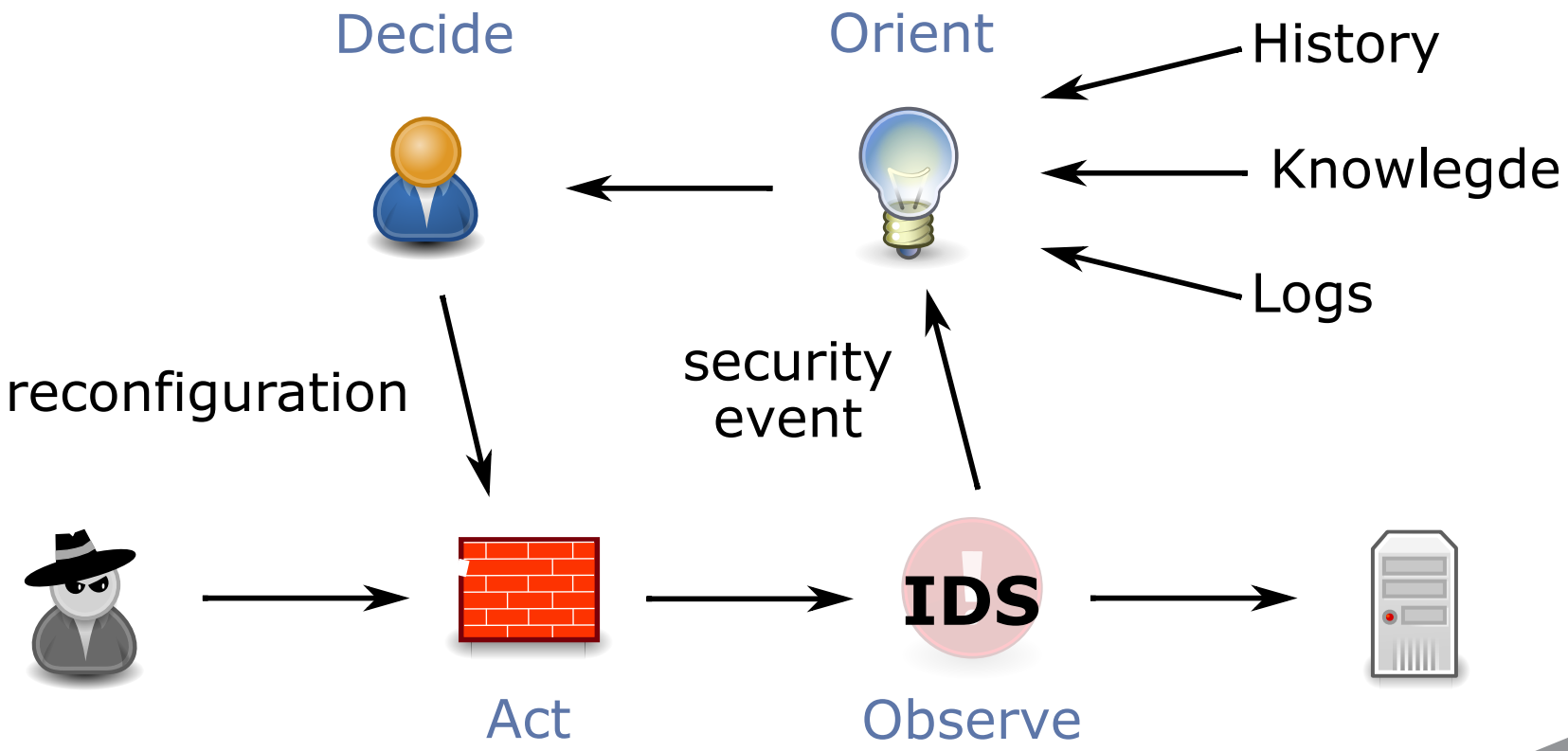
CSIRT-MU

Attack Response



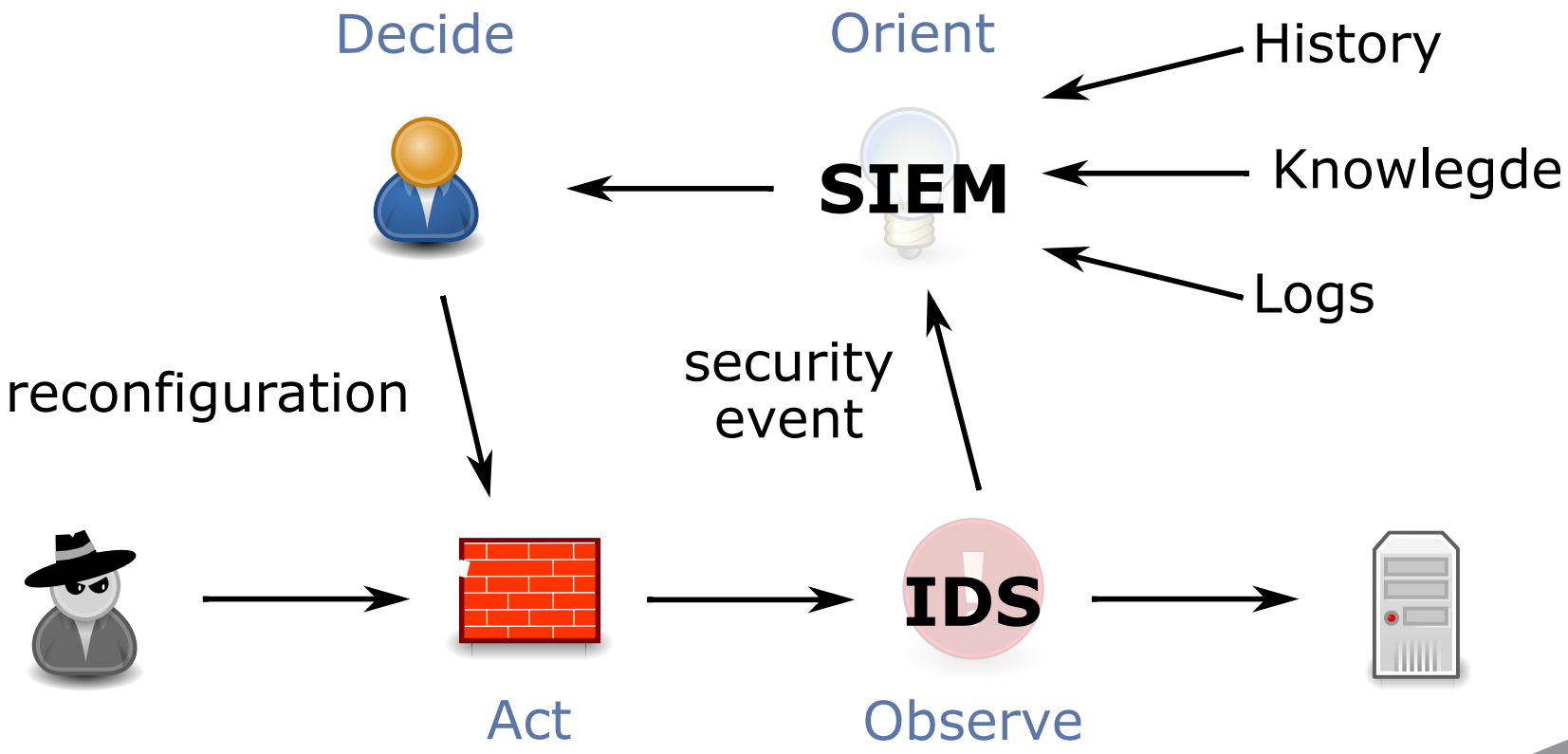
CSIRT-MU

Attack Response



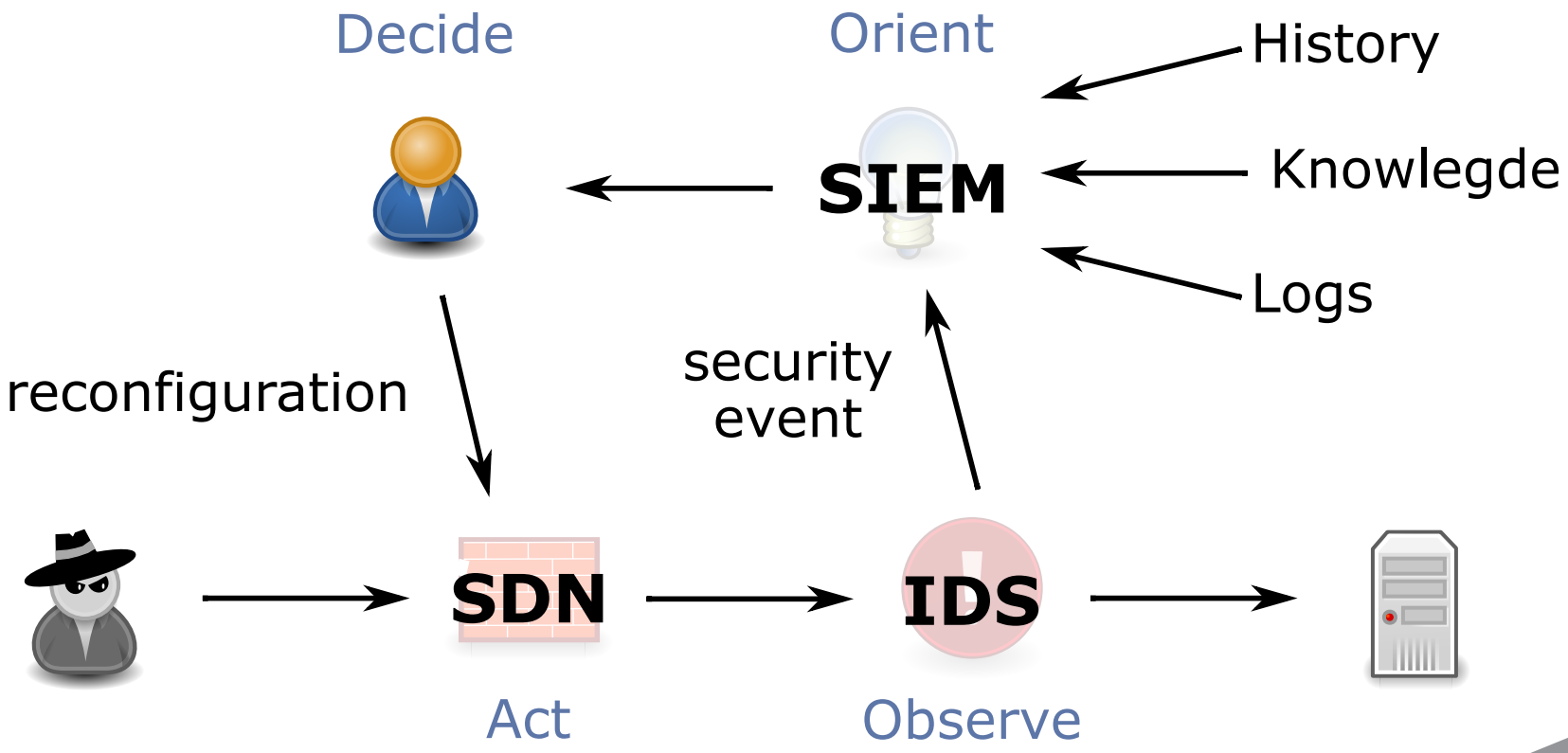
CSIRT-MU

Attack Response



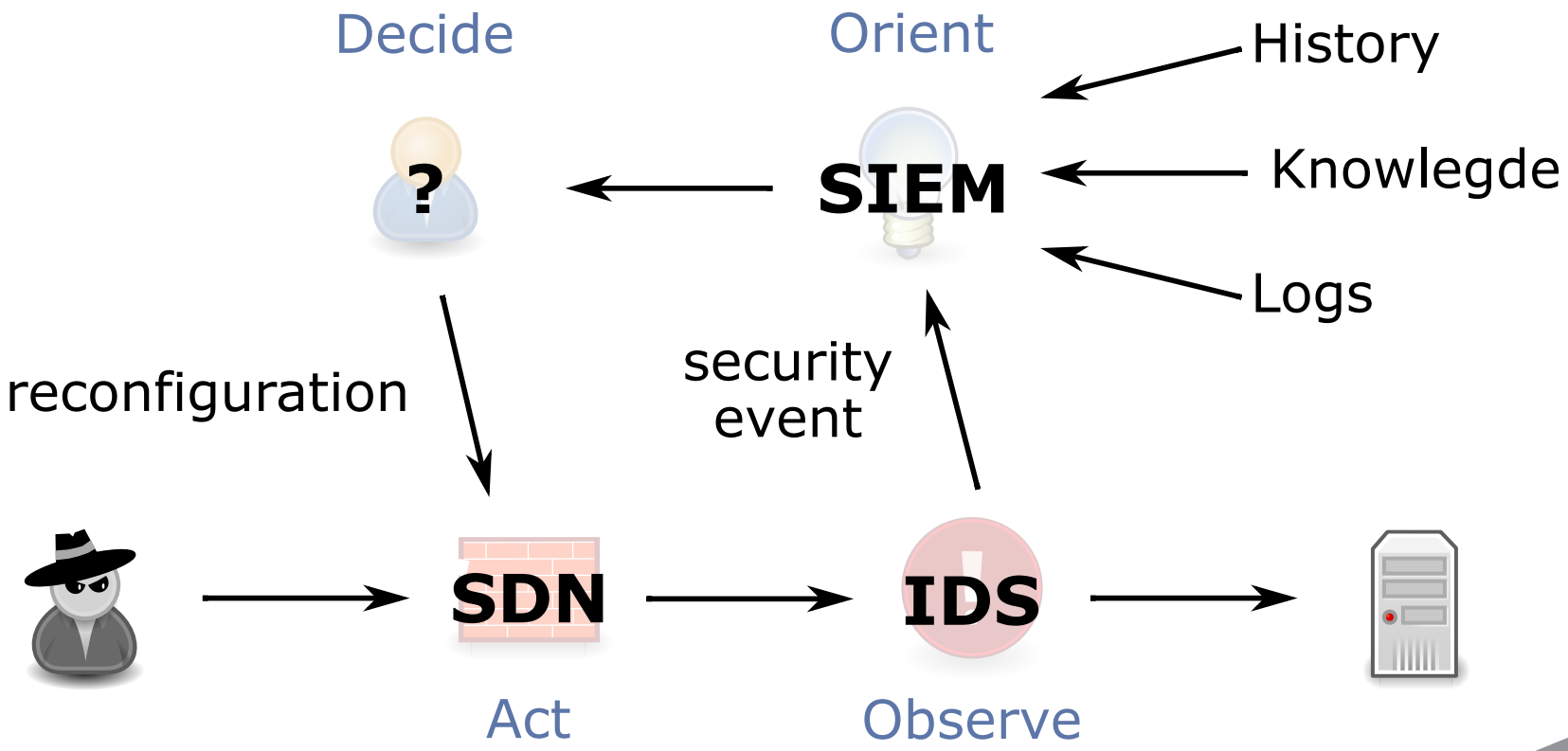
CSIRT-MU

Attack Response



CSIRT-MU

Attack Response



CSIRT-MU

Research Goal

Utilizing a model of interaction between an attacker and a defender to create more refined network defence strategy

Research Goal

Utilizing a model of interaction between an attacker and a defender to create more refined network defence strategy

- Select response based on received security events and knowledge of the network
- Include the attacker's motivation in the decision process

Research Topics

Research Question I

How can we model the interaction between an attacker and a defender?

Research Topics

Research Question I

How can we model the interaction between an attacker and a defender?

Research areas

- Modelling the interaction between an attacker and a defender
  - model the interaction
  - reasonable input parameters
  - optimal actions for defender and attacker
  - computational feasibility for large networks

Research Topics

Research Question II

How can we use the model to form a network defence strategy?

CSIRT-MU

Research Topics

Research Question II

How can we use the model to form a network defence strategy?

Research areas

- Network defence strategy
  - response action based on observed security alerts
  - unknown state of the network
  - unknown objective and past actions of an attacker

Research Topics

Research Question II

How can we use the model to form a network defence strategy?

Research areas

- Network defence strategy
  - response action based on observed security alerts
  - unknown state of the network
  - unknown objective and past actions of an attacker
- Strategy verification
  - KYPO - cloud-based testbed for simulation of cyber attacks

Research Topics

Research Question III

Can the human instinct and experience be included in the defence strategy?

Research Topics

Research Question III

Can the human instinct and experience be included in the defence strategy?

Research areas

- How can the response selection benefit from human input
  - **what** in the model or strategy can be made more accurate

Research Topics

Research Question III

Can the human instinct and experience be included in the defence strategy?

Research areas

- How can the response selection benefit from human input
  - **what** in the model or strategy can be made more accurate
- Merging the human intuition into decision output
  - **how** can we make it more accurate

Proposed Approach

Modelling the interaction between an attacker and a defender

- Game theory toolset
- Use existing or modified model
- Optimal attacker's and defender's strategy

Proposed Approach

Modelling the interaction between an attacker and a defender

- Game theory toolset
- Use existing or modified model
- Optimal attacker's and defender's strategy

Estimating model parameters

- Formal network description
  - the topology of the network
  - the hosts and services present in the network
  - the required levels of confidentiality, availability and integrity
  - interdependence of services
- Formal description of attacks and responses

Proposed Approach

Network defence strategy

- Maintain beliefs to manage uncertainty
  - the current state of the network
  - the attacker's past actions
  - the attacker's objective
- Precomputed optimal responses
- Best response action in a given situation

Proposed Approach

Strategy verification

- Cloud-based testbed for simulating cyber attacks
- Computer Security Incident Response Team (CSIRT) training exercises

Proposed Approach

Strategy verification

- Cloud-based testbed for simulating cyber attacks
- Computer Security Incident Response Team (CSIRT) training exercises

Adding human intuition to decision output

- Black-Litterman model in economy
- Formal description of human input
- Updating beliefs based on input

CSIRT-MU

Summary

- Network security requires an efficient autonomous system which would select a response action based on observed security events

CSIRT-MU

Summary

- Network security requires an efficient autonomous system which would select a response action based on observed security events
- Currently automated network defence systems react only in unambiguous situations and the rest of the events must be investigated by security experts

CSIRT-MU

Summary

- Network security requires an efficient autonomous system which would select a response action based on observed security events
- Currently automated network defence systems react only in unambiguous situations and the rest of the events must be investigated by security experts

CSIRT-MU

Summary

- Network security requires an efficient autonomous system which would select a response action based on observed security events
- Currently automated network defence systems react only in unambiguous situations and the rest of the events must be investigated by security experts
- We propose to model the interaction between an attacker and a defender to comprehend how the attacker's goals affect his actions and use the model as a basis for a more refined network defence strategy

THANK YOU FOR YOUR ATTENTION!

Jana Medková

medkova@ics.muni.cz