Anomaly Management using Complex Event Processing

Bastian Hoßbach and Bernhard Seeger

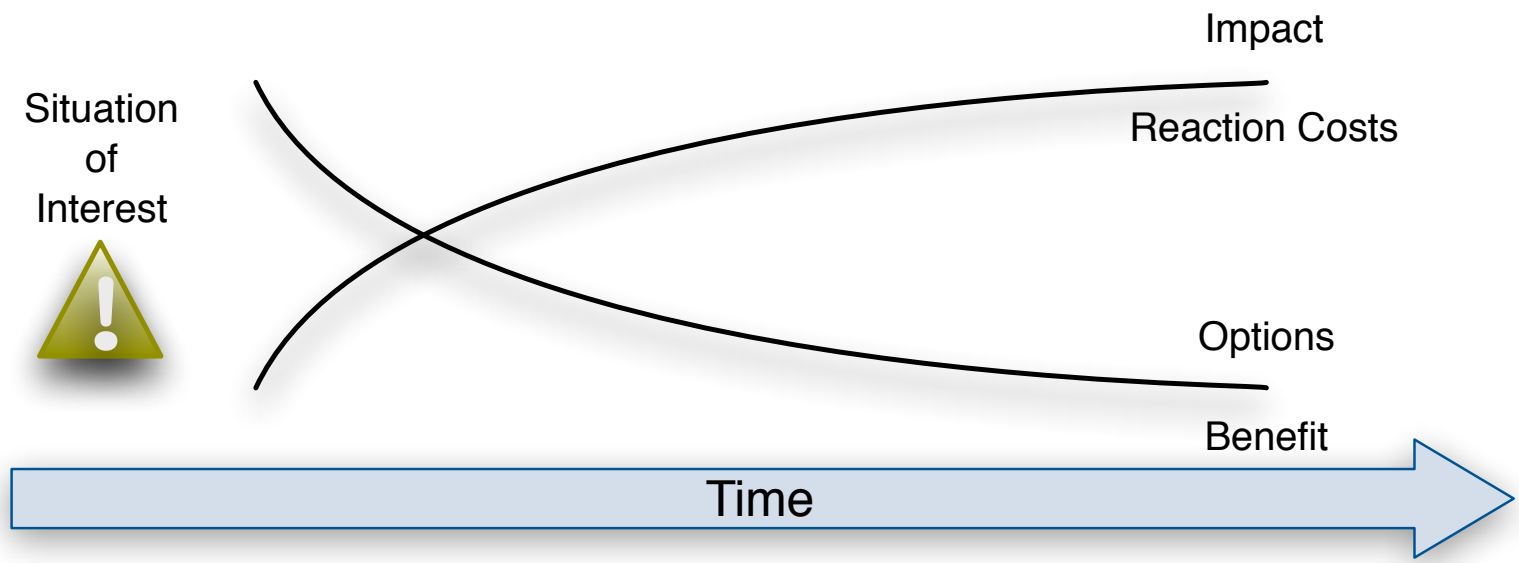
Philipps Universität Marburg

Int'l Conference on Extending Database Technology
Genoa, Italy – March 19, 2013

Agenda

- Introduction
- Enhanced complex event processing
- Conclusion

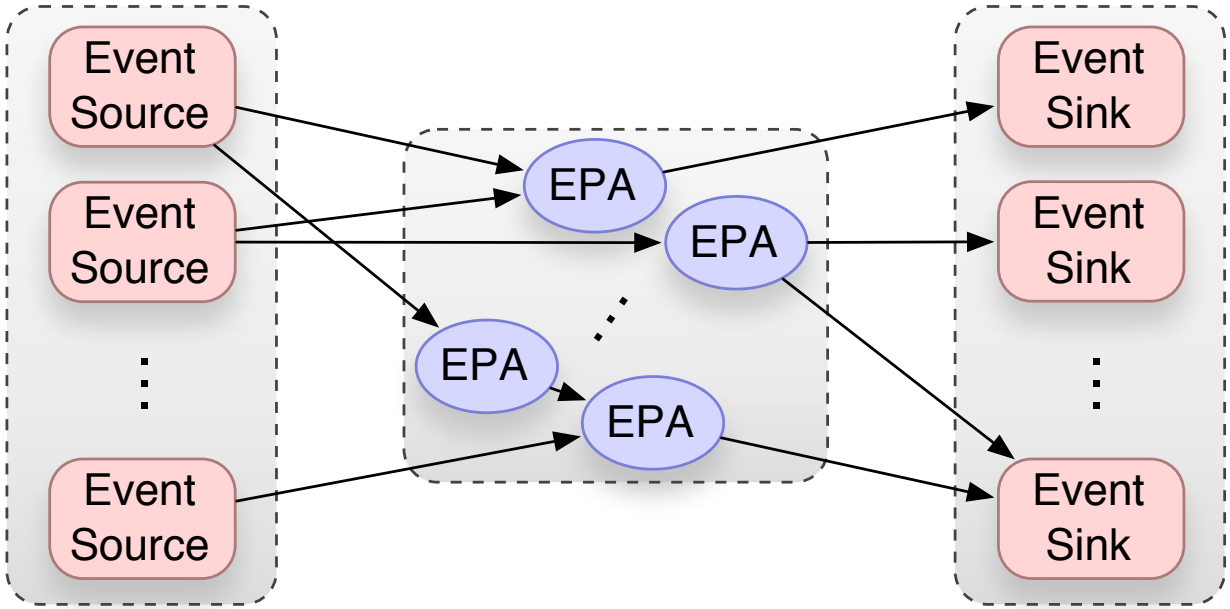
Why Complex Event Processing?



In order to be able to react on situations of interest (SOI) optimally, continuous monitoring in (near) real-time is necessary.

Philipps Universität Marburg

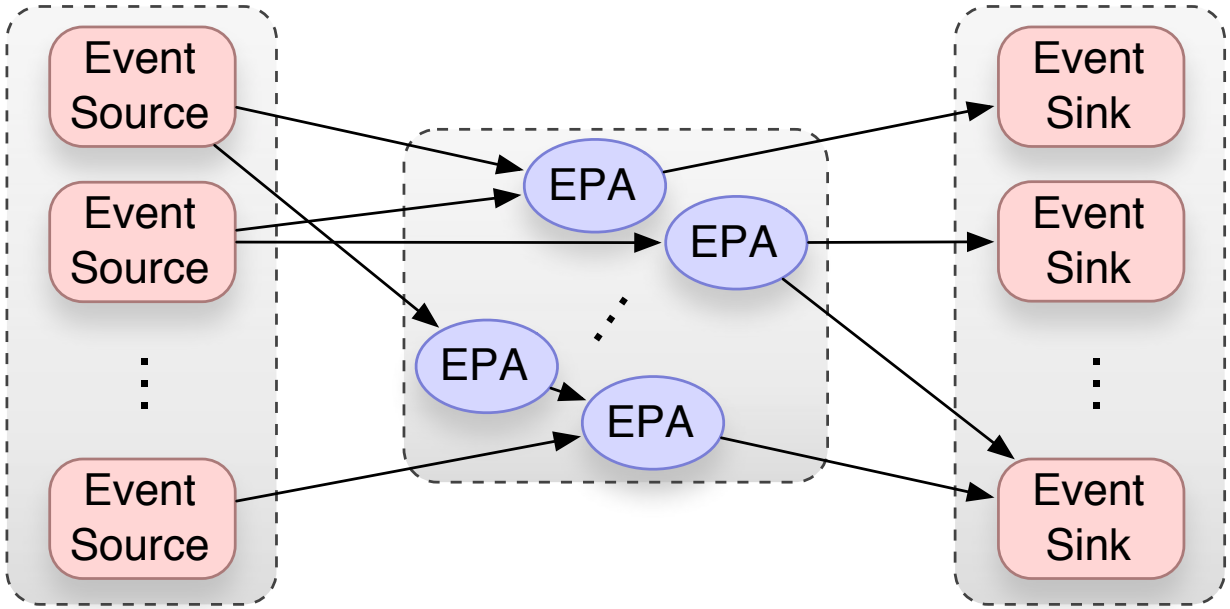
State of the Art: Static Complex Event Processing



Static event processing agents (EPA) support:

Philipps Universität Marburg

State of the Art: Static Complex Event Processing

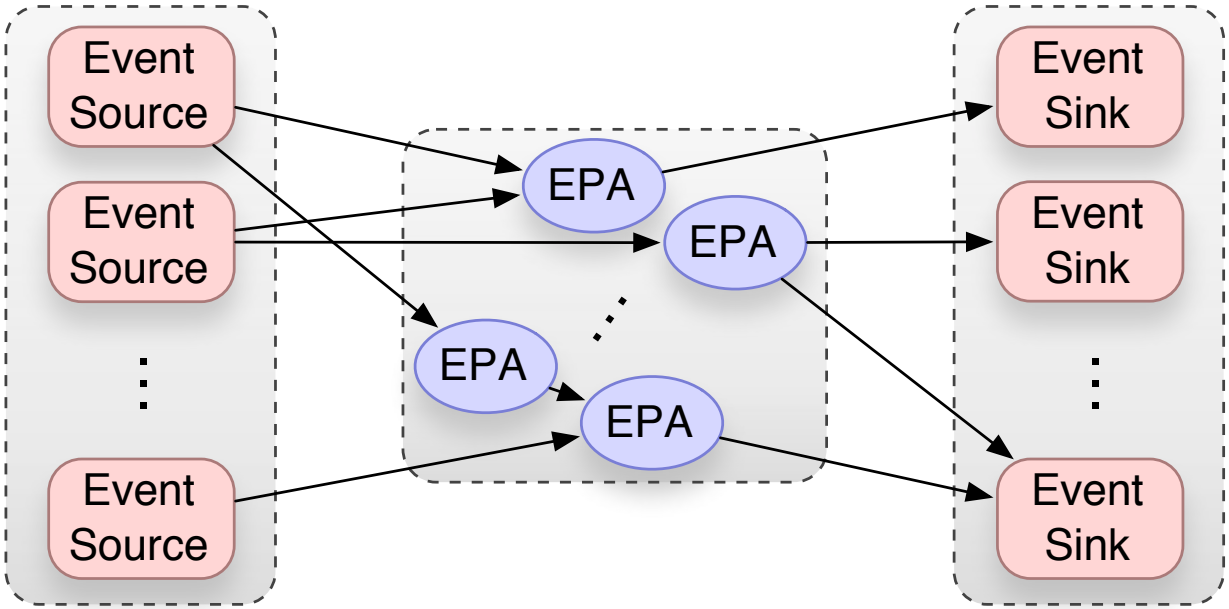


Static event processing agents (EPA) support:

- ✔ Signature-based monitoring

Philipps Universität Marburg

State of the Art: Static Complex Event Processing



Static event processing agents (EPA) support:

- ✔ Signature-based monitoring
- ✘ Anomaly-based monitoring

Philipps Universität Marburg

Motivation

What if there are billions of SOI?

What if there are unknown SOI?

What if there are context-sensitive SOI?

$\Rightarrow$ Signatures do not work. Anomaly management is needed!

Philipps Universität Marburg

Motivation: Patient Monitoring

Philipps Universität Marburg

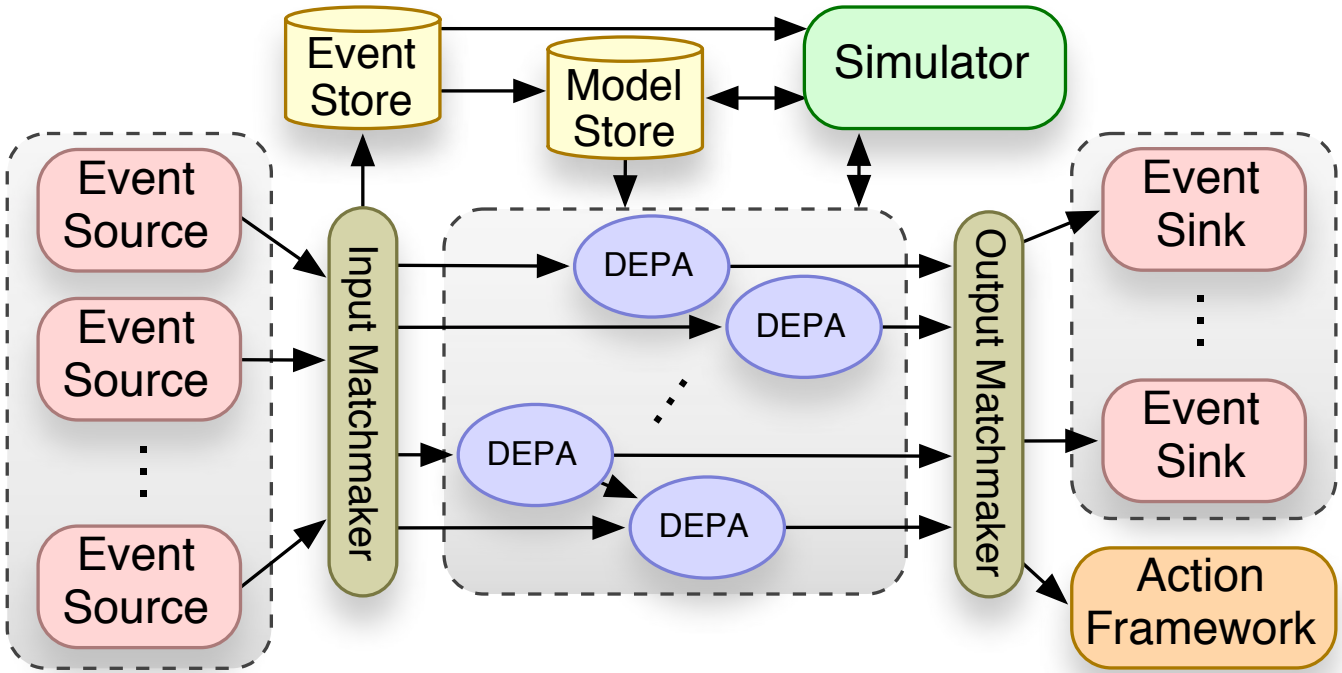
Motivation: Logistics

Philipps Universität Marburg

Motivation: Cyber Defense

Philipps Universität Marburg

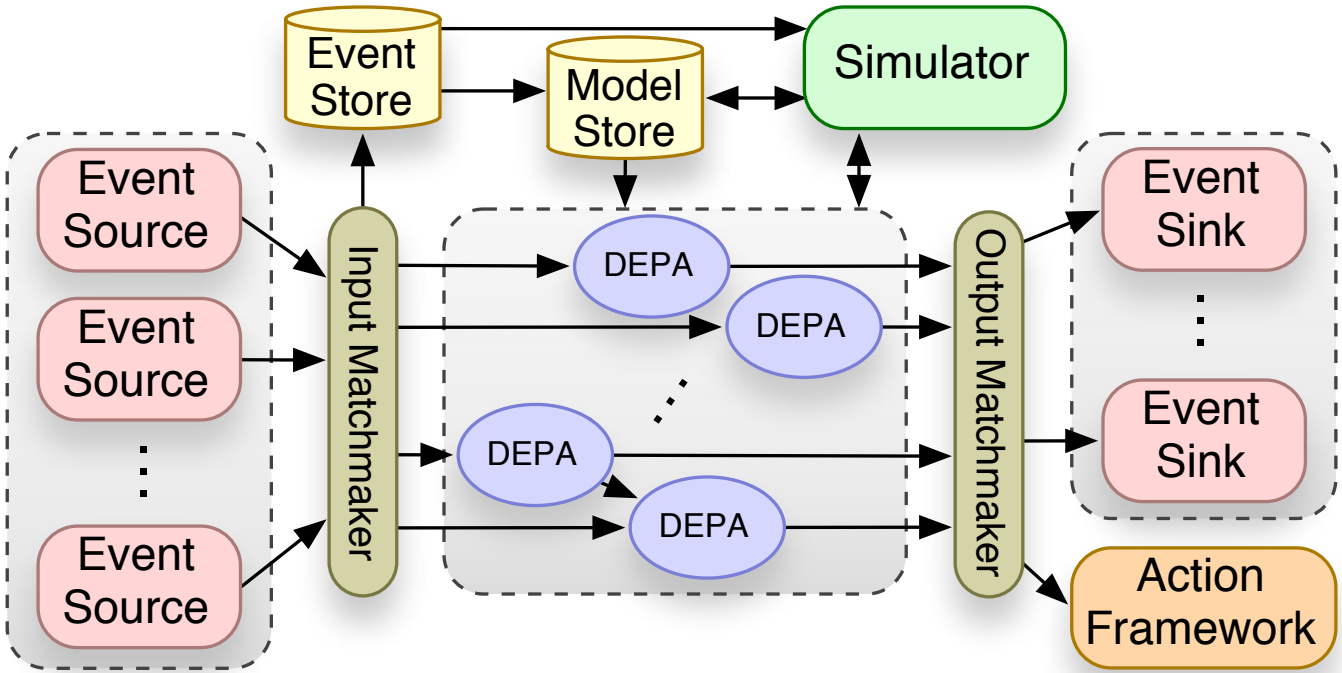
Flexible, Dynamic and Reactive CEP Infrastructures



Dynamic event processing agents (DEPA) support:

Philipps Universität Marburg

Flexible, Dynamic and Reactive CEP Infrastructures

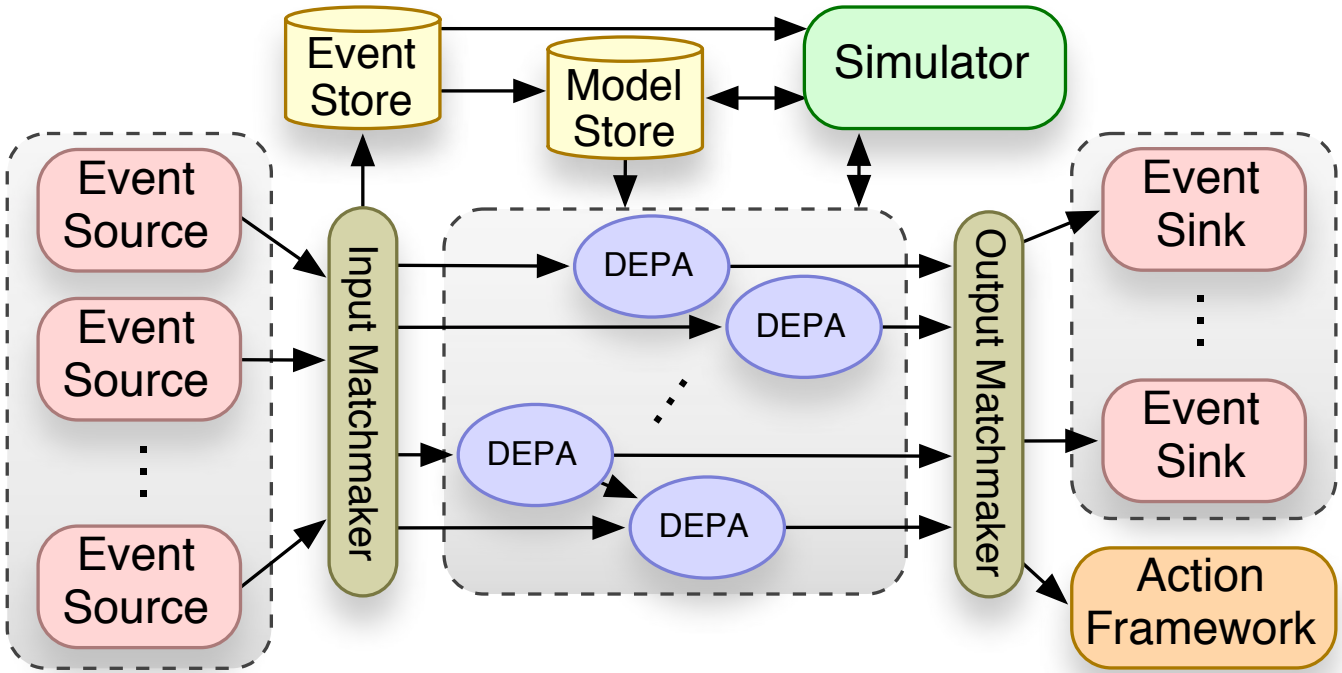


Dynamic event processing agents (DEPA) support:

- ✔ Signature-based monitoring

Philipps Universität Marburg

Flexible, Dynamic and Reactive CEP Infrastructures

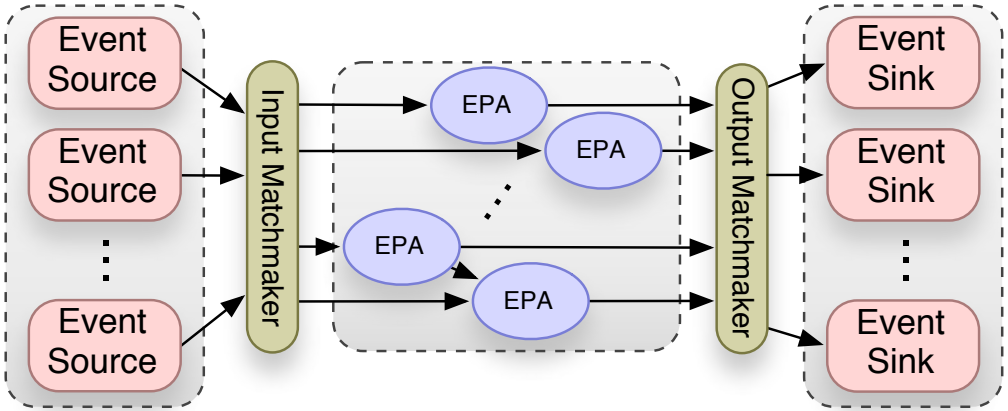


Dynamic event processing agents (DEPA) support:

- ✔ Signature-based monitoring
- ✔ Anomaly-based monitoring

Philipps Universität Marburg

Matchmakers



Flexible routing and transformation of events

⇒ Source/EPA independence

- Changes of event sources do not require adjustments of EPA

⇒ EPA/sink independence

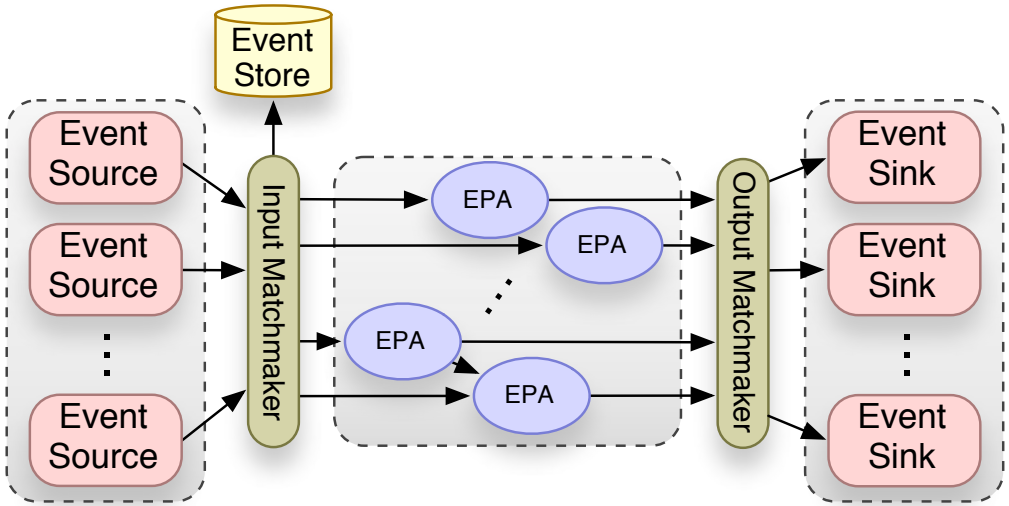
- Changes of EPA do not require adjustments of event sinks

⇒ Inter-EPA independence

- Changes of EPA do not require adjustments of the other EPA

Philipps Universität Marburg

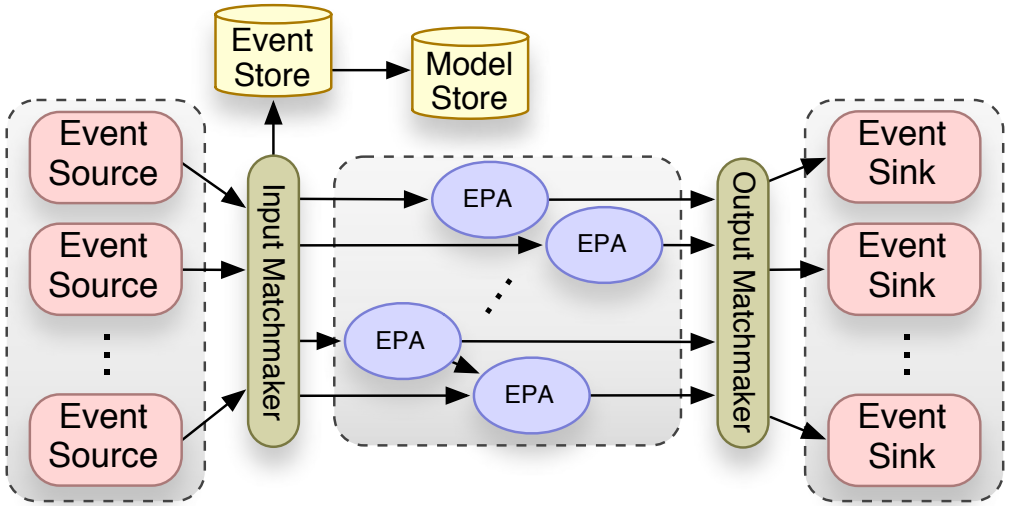
Event Store



- High-performance database to record and index events
- Optimized for fast writes and scalability
- Efficient support of temporal queries
- On-demand secondary indexes
- Fast garbage collection and compression of tenured events

Philipps Universität Marburg

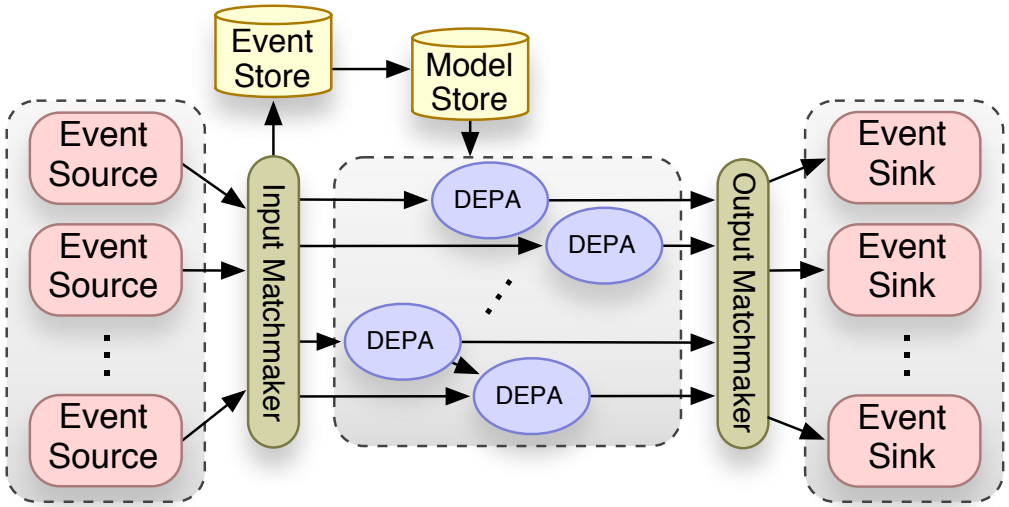
Model Store



- Management of models that describe normal behavior of monitored objects with respect to a certain context
- Models are selected, created and maintained on the basis of historical data from the event store

Philipps Universität Marburg

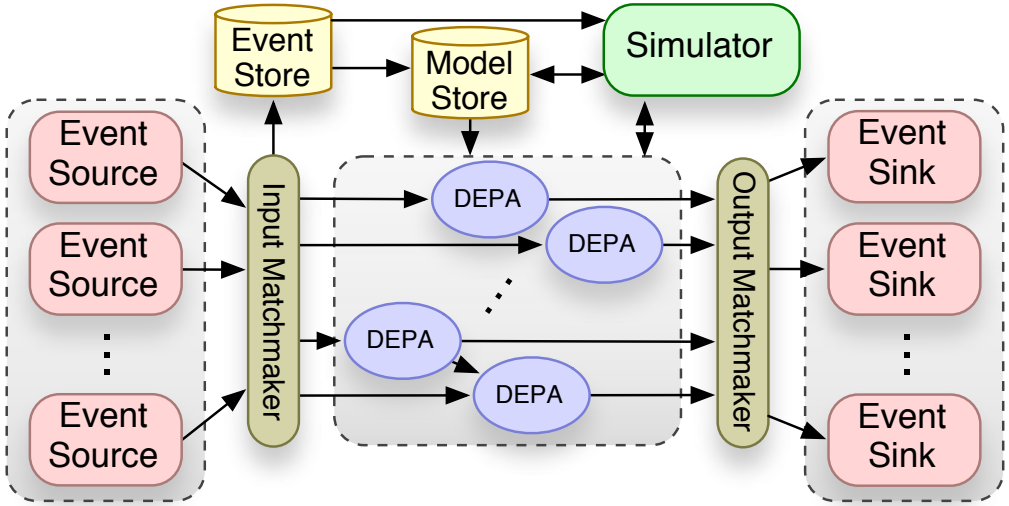
Dynamic EPA



- Models are used to create and maintain dynamic EPA (DEPA) that search for abnormalities in live event streams
- All detected anomalies are classified as potential situations of interest and forwarded to the output
- Because of fast and unpredictable context switches and updates of models, DEPA have to be able to be updated fast

Philipps Universität Marburg

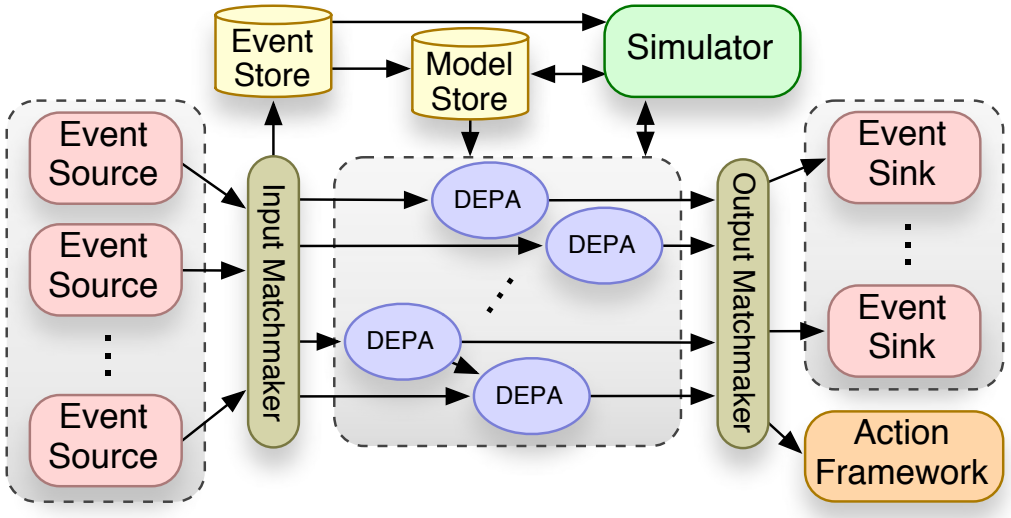
Simulator



- Isolated execution environment for testing, debugging and evaluating DEPA as well as models
- Real data is taken from the event store
- What-if analyses and continuous evaluations incrementally increase quality of DEPA

Philipps Universität Marburg

Action Framework



- Current CEP infrastructures are not reactive
  - Detected situations of interest are just reported
- Reactive CEP infrastructures need an action framework that allows to create actions and to define how they are triggered
- Provenance becomes very important

Philipps Universität Marburg

Conclusion

- State of the art CEP technology has multiple shortcomings
  - Not applicable in some important application domains
  - Many existing CEP-based monitoring systems can not develop their full potential
- CEP technology has to be improved and extended
  - Flexibility $\rightarrow$ Matchmakers
  - Dynamics $\rightarrow$ Dynamic EPA
  - Reactivity $\rightarrow$ Action Framework

Philipps Universität Marburg

Ongoing Work

- We are working on the outlined dynamic CEP infrastructure
- Target use-case: IT-security
  - Detection of SQL injections
  - Detection of intruders in post-exploitation phase
- Other active research projects are related to dynamic CEP
  - Active CEP
  - Semantic CEP

Philipps Universität Marburg

Thanks

- Dieter Gawlick for great discussions
- BMBF for funding ACCEPT

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Philipps Universität Marburg