SIEM approach for a higher level of IT security in enterprise networks

Kai-Oliver Detken[1], Thomas Rix[1], Carsten Kleiner[2], Bastian Hellmann[2], Leonard Renners[2]

1 DECOIT GmbH, Bremen, Germany
2 Trust@HsH Research Group - University of Applied Sciences and Arts, Hanover, Germany

September 25th 2015
IDAACS 2015
Warsaw, Poland

Outline

- Motivation
- Approach and Architecture
- Demonstration (Video)
- Conclusion

Motivation

Small and medium enterprises (SME)

- IT-Security requirements changed rapidly, especially due to mobile devices
- Most times only individual solutions implemented
- Not a sufficient security strategy

Security Information and Event Mangement (SIEM) Systems

- Solution integrating many information sources
- Can detect more complex attacks and offer better security
- Expensive deployment and maintenance
- → Not really applicable in SME

Our Contribution

- SIMU: A system providing many SIEM-like capabilities with focus on SME environments

SIMU in a Nutshell

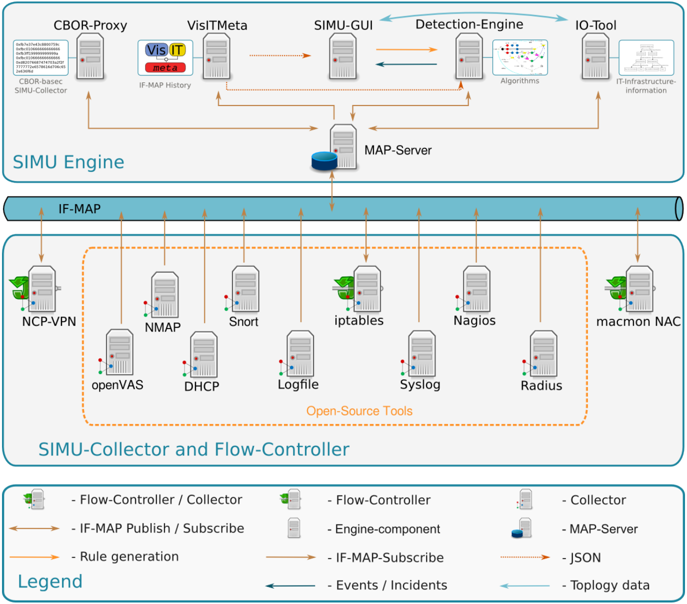
Data integration based on the IF-MAP specification

- Open specification to allow the exchange of information between arbitrary network components
- Homogeneous data format
- Many collecting and consuming clients (based on common and open source solutions)
- One central server

Automated Analysis and Reaction

- Central examination of the homogeneous data
- Possibility for automated enforcement
- Documentation and incident reporting

SIMU Architecture



Short demonstration

Video

Conclusion

Summary

- Integrated security management not easily available for SME - but needed!
- SIMU: SIEM-like system, especially for SME environments
- IF-MAP as the foundation
- Graph-based pattern matching for incident detection
- Ticket management and graph visualization for incident handling
- Possibility for automated actions

Thank you for your attention!

This work is financially supported by the German Federal Ministry of Education and Research (BMBF) within the SIMU project (grant no. 16KIS0045).

Further information:

`http://simu-project.de` `http://trust.f4.hs-hannover.de`