Combining NAC and SIEM functionality based on Open Source

K.-O. Detken · M. Jahnke (DECOIT GmbH)

C. Kleiner · M. Rohde (University of Applied Sciences Hanover)

Prof. Dr. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
detken@decoit.de

DECOIT®

Agenda

- Motivation
- Network Access Control (NAC) und Security Information and Event Management (SIEM)
- Architecture of CLEARER
- Data Exchange Format
- Integration of NAC systems
- Conclusions

Motivation

- Growing Interfaces to the Internet
  - Internet of Things (IoT)
  - Cloud Services
  - Industry 4.0
  - Medical IT devices/equipment
  - BYOD
- Isolated islands of IT security solutions
- In most cases: IT security components of different vendors are not working together
- Real-time analysing of all security data is not available

Network Access Control (NAC)

- Main issue: access control of systems and users for networks
- Tasks:
  - Identify foreign systems
  - Check security policies
    - Scan of installed applications
    - Scan of security updates
  - Allow or permit access via authorisation
  - Used policies to compare compliance
  - Shift end devices into quarantine zone if policies does not fit

Security Information and Event Management (SIEM)

- Main issue: overview about security status of the complete network
- Tasks:
  - Collection of security relevant information from the network
  - Assessment of the information
  - Prioritisation of the assessed information
  - Generation of messages about critical security issues
  - Provision of guidance regarding the handling of critical messages

CLEARER project

- CLEARER = Fulfill of compliance policies by processing of security events automatically
- CLEARER is a cooperation project within the German BMWi (ZIM) with the following partners:
  - DECOIT GmbH (coordinator and developer)
  - University of Applied Sciences of Hanover (research)
  - IT-Security@Work GmbH (compliance specialist)
  - macmon secure gmbh (NAC vendor)
- Associated partner:
  - ACHT:WERK (German vendor for SIEM-based Appliances)
  - rt-solutions (Consulting enterprise within SIEM area)
- The project has been started at May 2015 and will end at April 2017
- Project website: http://www.clearer-project.de

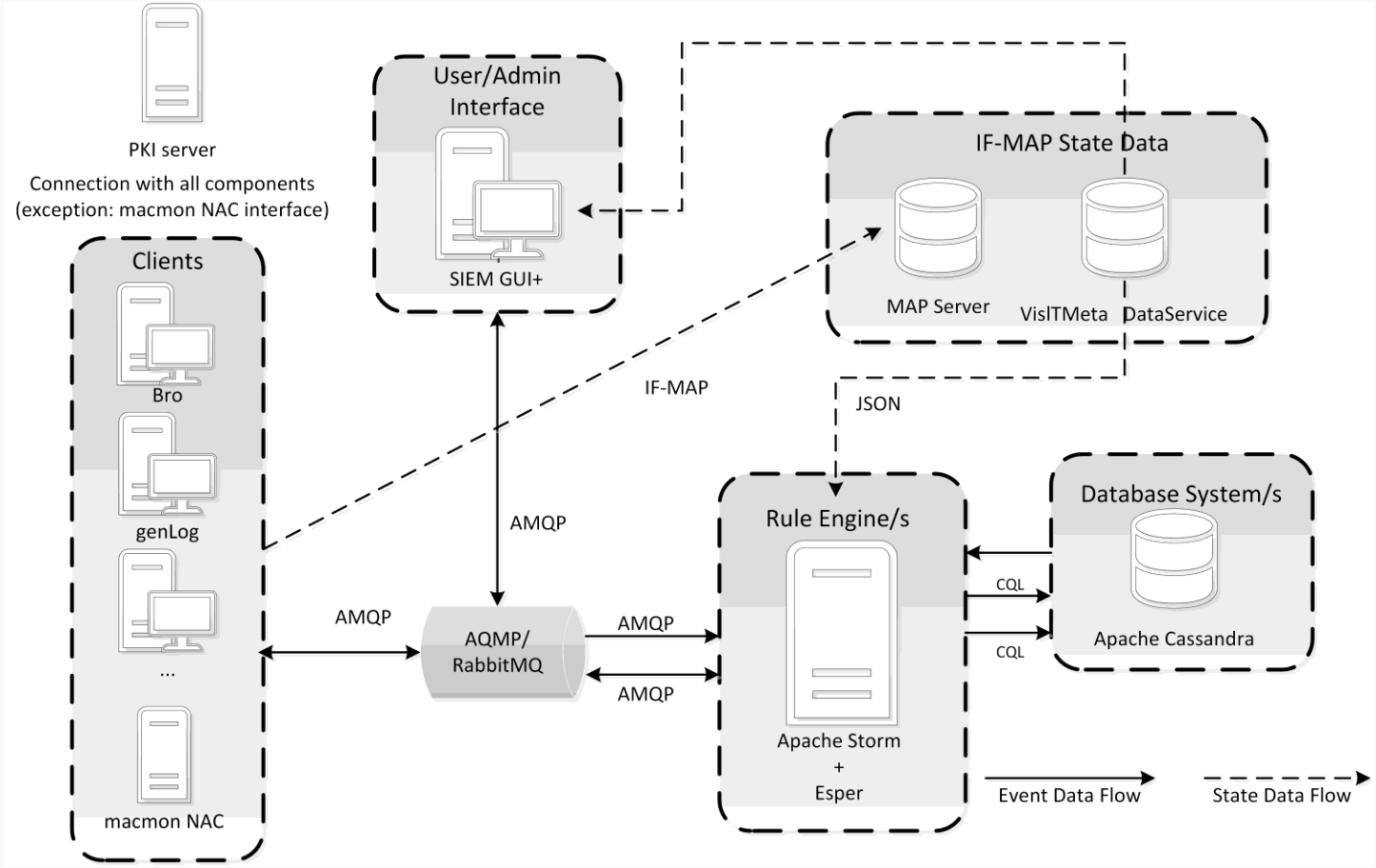
Focus of CLEARER

- Networking of NAC system, intrusion detection system (IDS), weak points scanner, log data, and SIEM system for policy enforcement of enterprise policies
  - Detect attacks and violations
  - Assess and prioritise attacks and violations
  - Initiate responses or inform administrators
  - Support administrators
- Conditioning of all collected data for simple forensic of occurred attacks
- Understandable and verifiable collection of all security-related information
- Simpler compliance control status for audits
- Main issue: Integration of SIEM functionality into NAC systems

Main goals of CLEARER

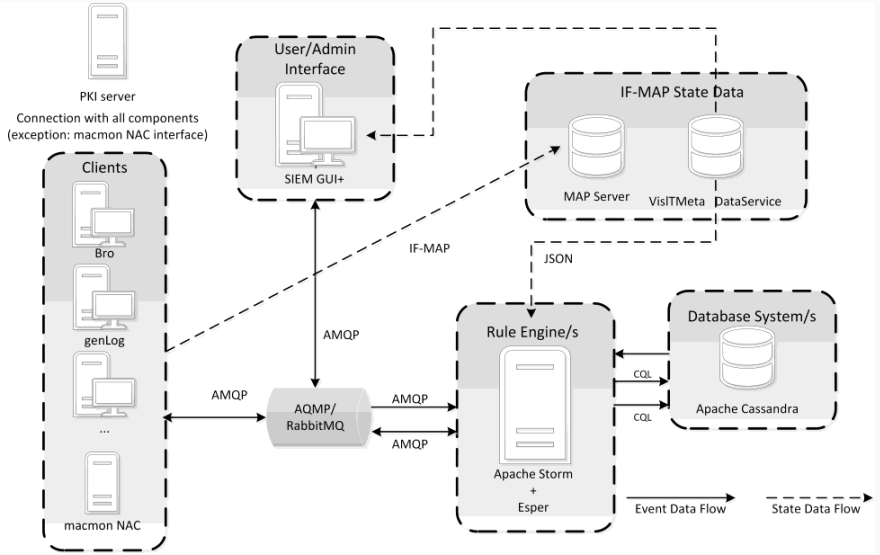
- Reduction of costs, by
  - the use of open source components
  - the use of horizontal scalability
  - the use of simple and central configuration
- The project has the following partial areas:
  - **Capturing of data:** includes information about the IT infrastructure, real-time data of components, services, and tools.
  - **Analysing of data:** processing of the information with big data approaches.
  - **Handling of messages:** aggregation of information for the escalation management and assessment.

Architecture of CLEARER



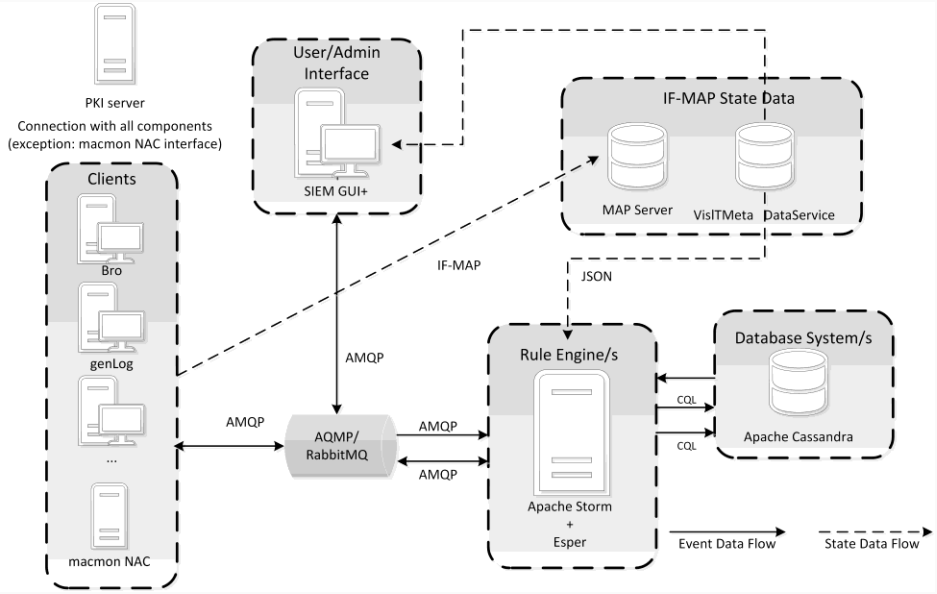
Components of CLEARER

- **SIEM GUI+:** main interface for administration and analysis. User rights management has been integrated.
- **Ticket system:** manage all tasks for the user and give hints of new alarms or events.
- **NAC system:** third party system for access control and regarding managing defined policies.
- **Banana auditing tool:** auditing tool to make log information visible efficiently.
- **Rule engine with Apache Storm and Esper:** event data has to be filtered (Apache Storm) before they will go through the correlation (Esper). Esper is also used as assessment engine because of its enormous correlation possibilities.
- **Apache Cassandra database system:** For logging of all relevant base data and events
- **IF-MAP** state data, including MAP server and VisITMeta data service
- **Bro:** open source network-monitoring, which inspects all traffic on a link in depth for malicious traffic.



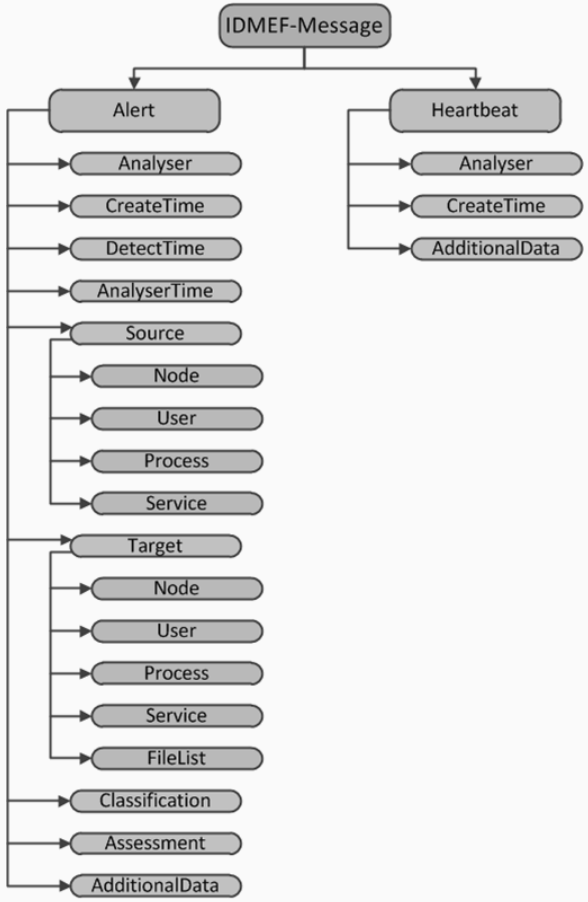
Architecture of CLEARER

- Central message queue for events with high performance and compliance processing
- Interface for Metadata Access Points (IF-MAP): Connection of status data, based on standards
- Splitting of events and status data (IF-MAP)
- Focus on high write performance of the database
- Events cannot be changed
- Self-Monitoring of the CLEARER system via compliance policies



Data Exchange Format

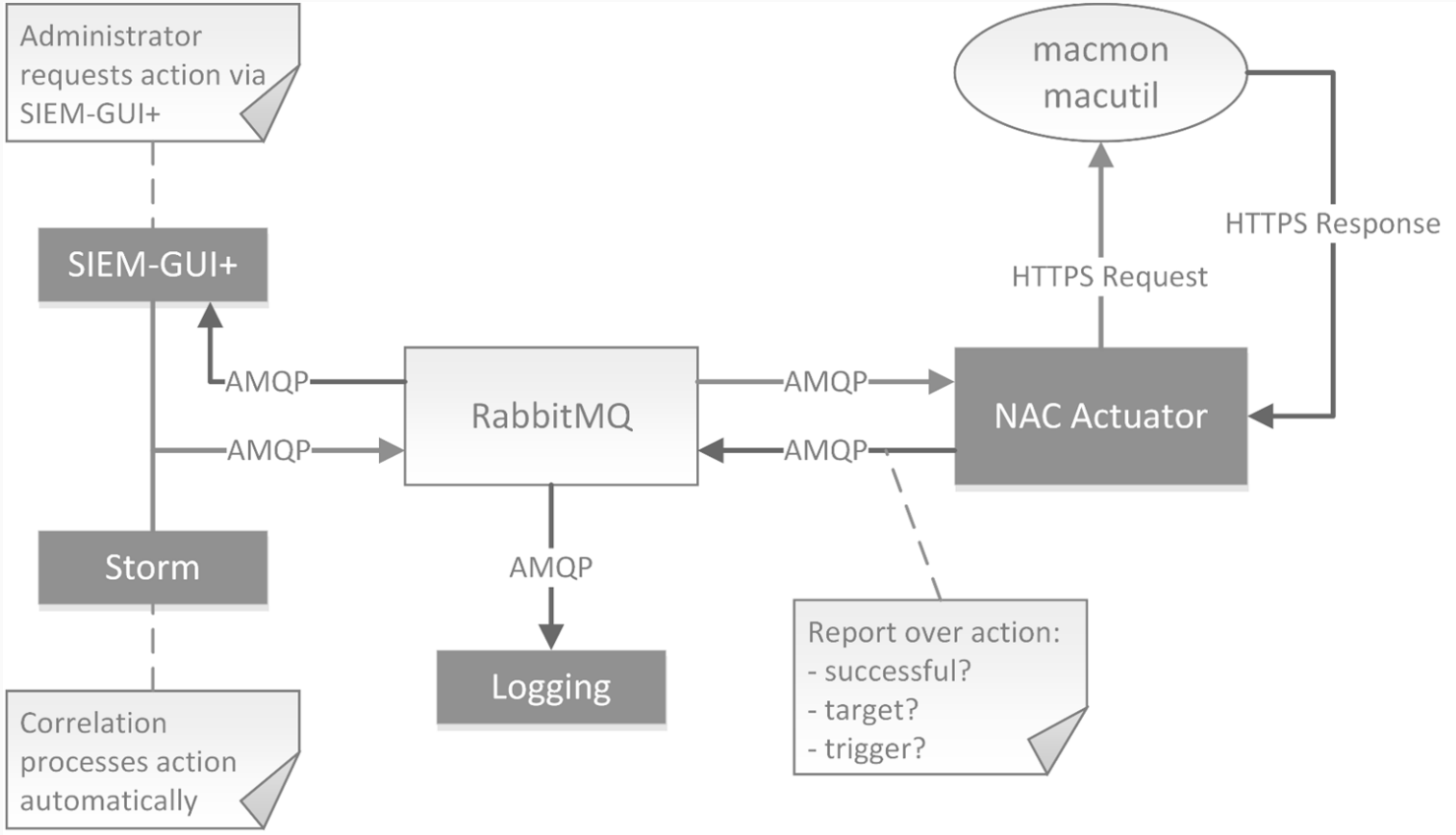
- As data exchange format for the event data between the different IF-MAP clients and the rule engine a standard format is necessary
- It has to distinguish between the format for the content and the format for the serialization
  - As content format the project uses the Intrusion Detection Message Exchange Format (IDMEF)
  - Concise Binary Object Representation (CBOR) has been chosen for the serialization format (RFC-7049)



Scenario example

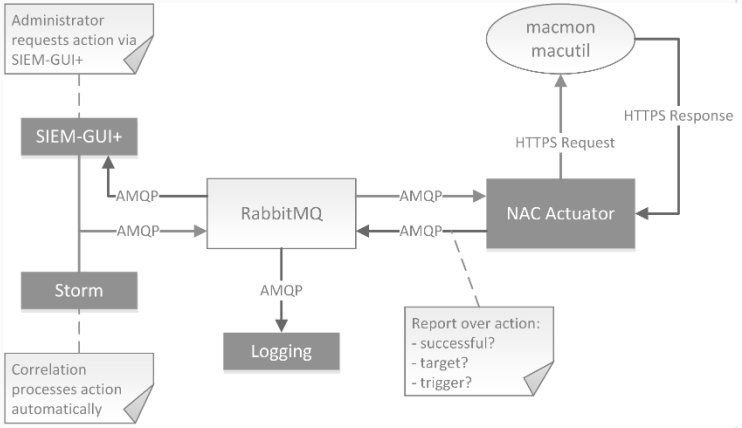
- Identify of an IT security weakness and priority
  - Vulnerability scans execute continuously
  - Assessment of vulnerability results by infrastructure information
  - Visibility of vulnerable events at the SIEM-GUI interface
  - After 30 days vulnerability scan executes again
  - Vulnerable event is still available → higher priority, adaptation of the removal time, and E-Mail with a request to administrator
  - Logging for compliance traceability

Integration of NAC system



3rd party integration

- Interface to NAC systems is necessary for the data exchange between SIEM and NAC
  - macutil tool for macmon secure
  - REST-API interface
- The tool macutil can be accessed by command line interface (CLI) or https (TLS)
- For the communication with arbitrary NAC systems, the functionality is encapsulated within a NAC actuator
- This actuator handles the incoming requests and transforms them into a format (e.g. https request), which can be used by the connected interfaces
- Because of limitations of macutil and the integration of other NAC systems, the project will use REST-API interface (future work)



Conclusions

- CLEARER includes a SIEM-based architecture with direct connectivity to existing NAC systems (e.g. macmon secure)
- One main goal of the project CLEARER is to fulfill IT compliance standards regarding security for small and medium-sized enterprises (SME) easily
- Another goal is to proof these compliance standards to different authorities
- Additionally, the main focus for all used components was on open source software to limit license costs and to use open interfaces
- Regarding the amount of data and its access patterns, which the new architecture has to handle, new database approaches are used
- In addition, auditing features for all changes on database content are required for compliance reasons

Thank you for your attention!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

https://www.decoit.de
info@decoit.de