Intelligent Anomaly Detection with SIEM Systems in Information Technology (IT) and Operational Technology (OT) environments

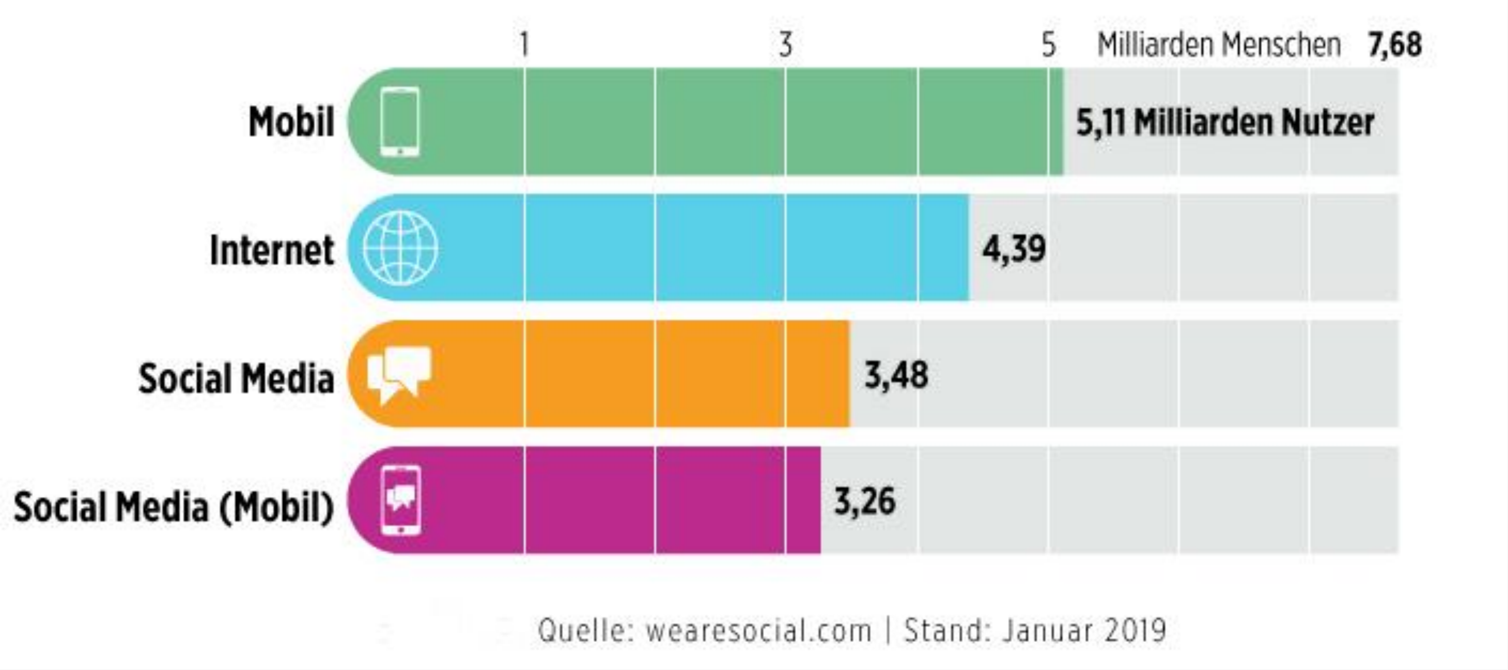
Prof. Dr. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
detken@decoit.de

Agenda

- Growing of Internet
- IT and OT networks
- Security tasks
- IT security development
- Use of monitoring systems
- What we need for more security
- GLACIER project with anomaly detection
- Conclusions

Internet is further growing

- The number of Internet users is growing worldwide by eleven new users per second or one million per day:



Quelle: wearesocial.com | Stand: Januar 2019

DECOIT®
0110010001100101011000110110111101101001011110100

IT and OT grow together

- IT and OT network infrastructures are growing too
- Both networks worked in the past in a peaceful coexistence
- By the growing of the Internet this coexistence changed
- Additional it gives new Interfaces to the Internet
  - Internet of Things (IoT)
  - Cloud Services
  - Industry 4.0
  - Medical IT devices/equipment
  - BYOD
- At the end of this year 50 billion devices(!) will be connected by the Internet
- Security is one of the main tasks we have to solve

Security tasks

- All these networked devices must be managed and secured – but, who is responsible?
- Operational Technology (OT) is hardware and software that detects and causes change by directly monitoring and/or controlling physical devices, processes and events in the enterprise (see Gartner)
- But, OT was previously concentrated on production and industrial plants – but usually in closed systems, without connection to the Internet
- On the other hand, IT has far more experience with the Internet and data security

IT security development

- Access Control Lists (ACL) have been set up on the routers and switches for security purposes
- Static filters could not be maintained, however, which is why they were later implemented in firewalls depending on the connection (keyword: stateful inspection)
- Application ports were blocked without analyzing the traffic
- Intrusion Detection Systems (IDS) have been introduced for anomaly detection without considering the administrative effort
- Anti-virus and anti-spam systems are used on the basis of pure pattern recognition

.DECOIT®
0110010001100101011000110110111101101001011101 00

Most cyber-attacks in ICS networks (BSI study from 2019)

1. Infiltrating malware via removable media and external hardware ↑
2. Infection with malware via Internet and Intranet ↑
3. Human mistakes and sabotage ↑↑
4. Compromise of extranet and cloud components ↑↑
5. Social Engineering and Phishing ↓
6. (D)DoS attacks ↑↑
7. Internet-connected control components →
8. Break-in via remote maintenance accesses →
9. Technical misconduct and force majeure ↓
10. Compromise of smartphones in the production environment →

IT and OT infrastructures

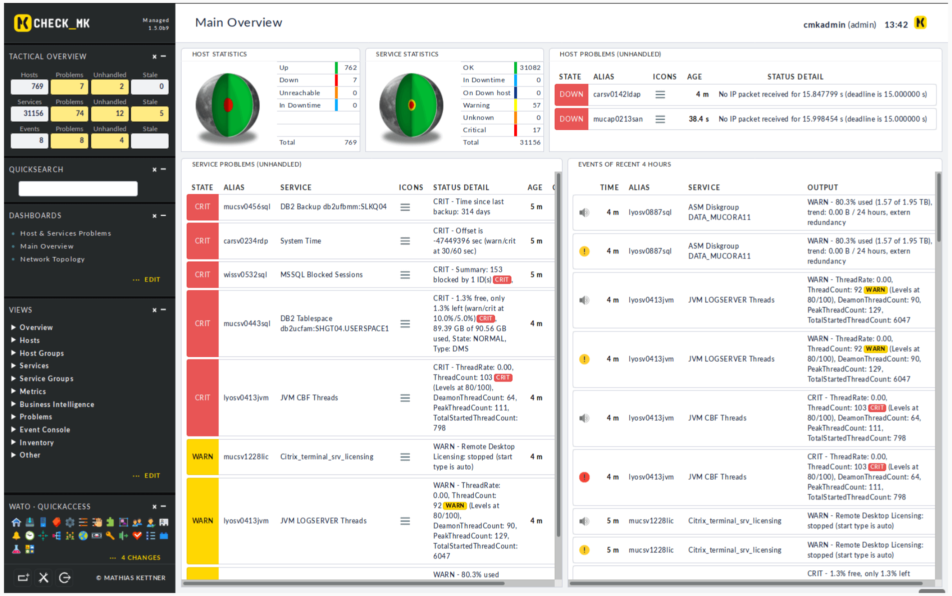
- IT infrastructures therefore have a 10-year lead in the field of IT security
- A close cooperation between OT and IT would therefore be the ideal solution
- However, both areas still work side by side rather than together
- Growing integration of classic information technology (IT) and operational technology (OT) creates risks of its own
- A further problem is, that isolated islands of IT security solutions still exists
- In most cases: IT security components of different vendors are not working together
- Real-time analysing of all security data is not available

Use of monitoring systems

- Evolution of monitoring and regulation systems:
  - **Network Monitoring:** Monitoring of availability and network documentation
  - **Network Access Control (NAC):** Monitoring of access control and end device documentation
  - **Security Information and Event Management (SIEM):** Monitoring of IT security and correlation of events (incidents)
- Goal: more security in IT and (maybe) OT networks

Network Monitoring

- Main issue: Monitoring of services and server systems and collection of availability statistics
- Tasks:
  - Integration of network and server components
  - Monitoring of services (services)
  - Escalation management for alarm messages (SMS, e-mail)
  - Summary of alarm messages
  - Differentiation of different priorities



CHECK_MK Managed 1.5.0b9

TACTICAL OVERVIEW

Hosts	Problems	Unhandled	Stale
769	7	2	0
Services	**Problems**	**Unhandled**	**Stale**
31156	74	12	5
Events	**Problems**	**Unhandled**	**Stale**
8	8	4	

QUICKSEARCH

DASHBOARDS
- Host & Services Problems
- Main Overview
- Network Topology

... EDIT

VIEWS
- Overview
- Hosts
- Host Groups
- Services
- Service Groups
- Metrics
- Business Intelligence
- Problems
- Event Console
- Inventory
- Other

... EDIT

WATO · QUICKACCESS

... 4 CHANGES

© MATHIAS KETTNER

Main Overview

cmkadmin (admin) 13:42

HOST STATISTICS

Up	762
Down	7
Unreachable	0
In Downtime	0
Total	769

SERVICE STATISTICS

OK	31082
In Downtime	0
On Down host	0
Warning	57
Unknown	0
Critical	17
Total	31156

HOST PROBLEMS (UNHANDLED)

STATE	ALIAS	ICONS	AGE	STATUS DETAIL
DOWN	carsv0142ldap	≡	4 m	No IP packet received for 15.847799 s (deadline is 15.000000 s)
DOWN	mucap0213san	≡	38.4 s	No IP packet received for 15.998454 s (deadline is 15.000000 s)

SERVICE PROBLEMS (UNHANDLED)

STATE	ALIAS	SERVICE	ICONS	STATUS DETAIL	AGE
CRIT	mucsv0456sql	DB2 Backup db2ufbmm:SLKQ04	≡	CRIT - Time since last backup: 314 days	5 m
CRIT	carsv0234rdp	System Time	≡	CRIT - Offset is -47449396 sec (warn/crit at 30/60 sec)	5 m
CRIT	wissv0532sql	MSSQL Blocked Sessions	≡	CRIT - Summary: 153 blocked by 1 ID(s) CRIT,	5 m
CRIT	mucsv0443sql	DB2 Tablespace db2ucfam:SHGT04.USERSPACE1	≡	CRIT - 1.3% free, only 1.3% left (warn/crit at 10.0%/5.0%) CRIT, 89.39 GB of 90.56 GB used, State: NORMAL, Type: DMS	4 m
CRIT	lyosv0413jvm	JVM CBF Threads	≡	CRIT - ThreadRate: 0.00, ThreadCount: 103 CRIT (Levels at 80/100), DeamonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798	4 m
WARN	mucsv1228lic	Citrix_terminal_srv_licensing	≡	WARN - Remote Desktop Licensing: stopped (start type is auto)	4 m
WARN	lyosv0413jvm	JVM LOGSERVER Threads	≡	WARN - ThreadRate: 0.00, ThreadCount: 92 WARN (Levels at 80/100), DeamonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047	4 m
				WARN - 80.3% used	

EVENTS OF RECENT 4 HOURS

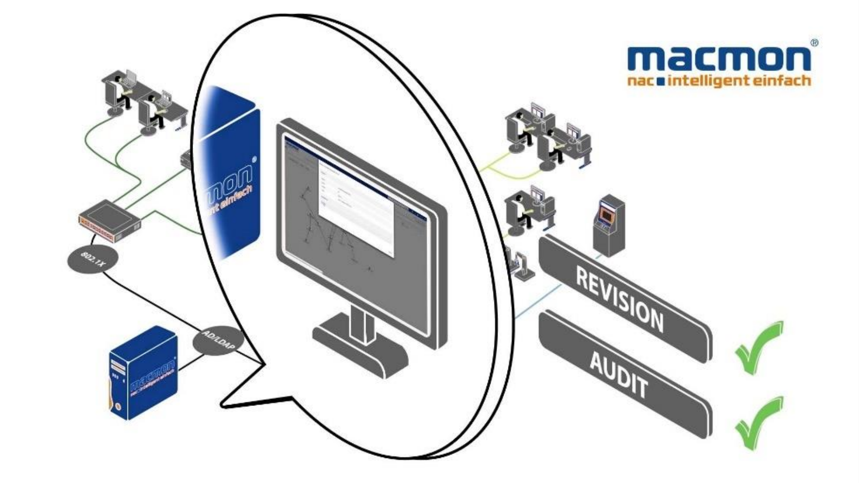
	TIME	ALIAS	SERVICE	OUTPUT
🔈	4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORA11	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
!	4 m	lyosv0887sql	ASM Diskgroup DATA_MUCORA11	WARN - 80.3% used (1.57 of 1.95 TB), trend: 0.00 B / 24 hours, extern redundancy
🔈	4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 WARN (Levels at 80/100), DeamonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
!	4 m	lyosv0413jvm	JVM LOGSERVER Threads	WARN - ThreadRate: 0.00, ThreadCount: 92 WARN (Levels at 80/100), DeamonThreadCount: 90, PeakThreadCount: 129, TotalStartedThreadCount: 6047
🔈	4 m	lyosv0413jvm	JVM CBF Threads	CRIT - ThreadRate: 0.00, ThreadCount: 103 CRIT (Levels at 80/100), DeamonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
!	4 m	lyosv0413jvm	JVM CBF Threads	CRIT - ThreadRate: 0.00, ThreadCount: 103 CRIT (Levels at 80/100), DeamonThreadCount: 64, PeakThreadCount: 111, TotalStartedThreadCount: 798
🔈	5 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
!	5 m	mucsv1228lic	Citrix_terminal_srv_licensing	WARN - Remote Desktop Licensing: stopped (start type is auto)
				CRIT - 1.3% free, only 1.3% left

Network Monitoring solutions

- Nagios:
  - Quasi standard of today's monitoring solutions
  - Offers a collection of modules for monitoring the network, hosts and specific services
- Icinga:
  - Released in 2009 as a fork from Nagios
  - Reason was the sluggish development and missing support
  - The web interface has been modernized
- Check_MK:
  - Originally since 2009 pure Add-On for Nagios
  - Today own powerful core (complete monitoring solution)
  - Much more scalable, better performance and easier to configure

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

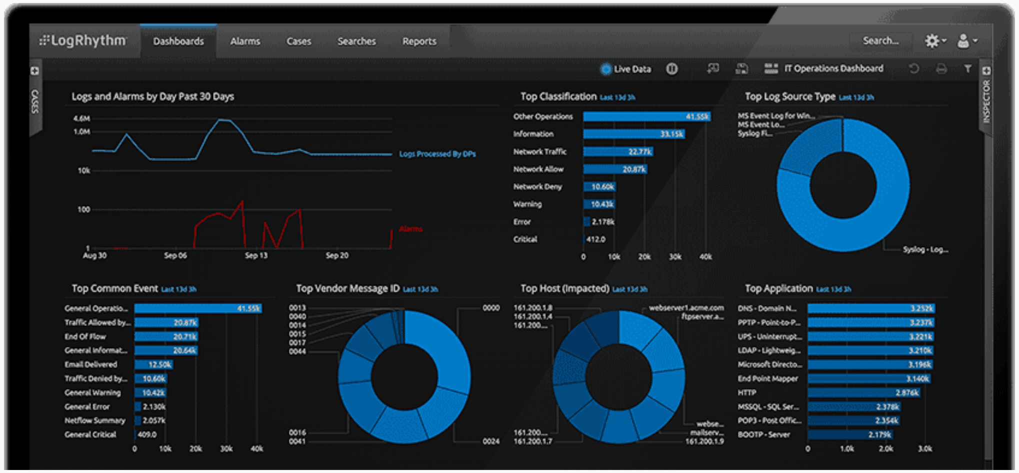


NAC solutions

- macmon secure:
  - BSI certified NAC solution
  - Independent of manufacturer
  - Mixed operation with and without 802.1X
  - Enables compliance rules to be applied
- Packet Fence:
  - Open Source solution without license costs
  - Similarly powerful as manufacturer solutions
  - Detection of network anomalies, proactive scans, isolation of problematic end devices

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



SIEM solutions

- LogRhythm:
  - Efficient Pattern Matching
  - Dashboard is customizable
  - Probability for “false positives” can be specified
- OSSIM:
  - Has been developed as an open source solution
  - Has been adopted from the manufacturer AlienVault
  - Integrates other open source solutions: OpenVAS, Snort, Nagios, Munin etc.

IT security builds on open source

- Many proprietary manufacturers of IT security products use open source solutions
- In some areas, open source solutions have even become established (quasi standard)
    - VPN: OpenVPN
    - Firewall: pfSense / OPNsense
    - Anti-virus/anti-spam protection: ClamAV / rspamd
    - Proxy: Squid
    - Intrusion detection systems: Snort / Suricata
    - Monitoring: Nagios / Icinga / Check_MK

What we need for more security

- Cooperation of different manufacturers / vendors of security solutions
- Understanding IT and OT networks as a common infrastructure
- Use more open source to promote open standards and interfaces
- Provide security solutions with more intelligence, since currently only well-known security patterns are searched for
- Make the handling of such systems easier, so that not only security experts can use them

Future: GLACIER project

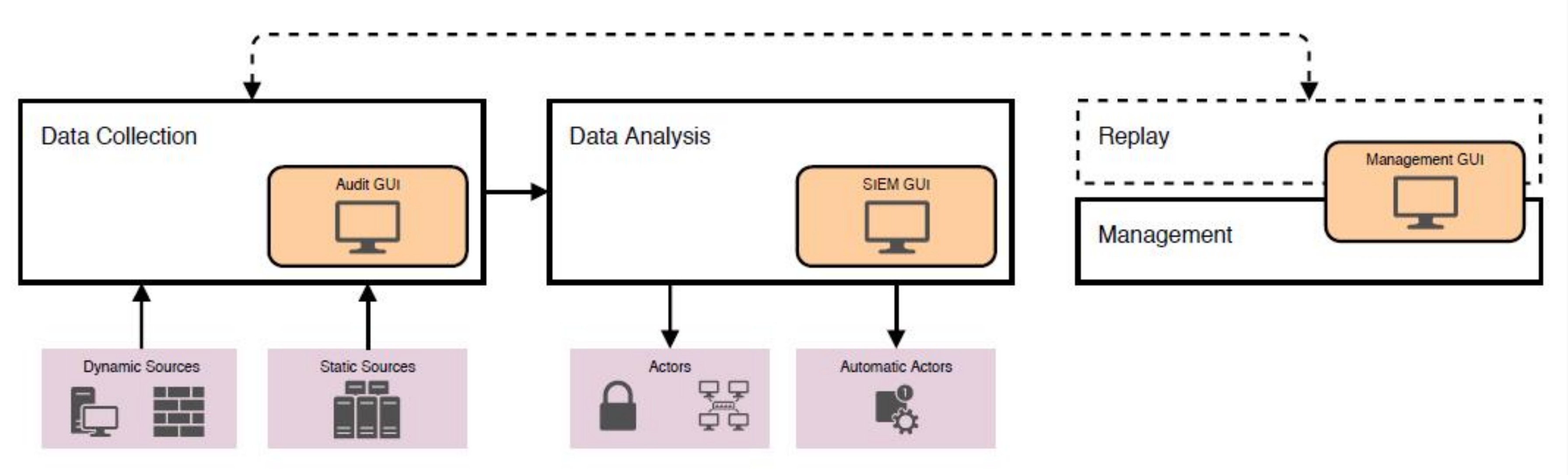
- GLACIER = Intrusion detection via multi-dimensional analysis of security data streams
- GLACIER is a cooperation project within the German BMBF with the following partners:
  - DECOIT GmbH (coordinator and developer)
  - University of Applied Sciences of Hanover (research)
  - rt-solutions.de GmbH (developer)
- Associated partner:
  - PLATE (German major supplier for office supplies)
  - hanseWasser (KRITIS operators in the field of waste water)
- The project has been started at April 2019 and will end at September 2021
- Project website: http://www.glacier-project.de

Focus of GLACIER

- The goal of a SIEM system should be to be able to correlate protocols from heterogeneous sources in order to provide the Security Operation Center (SOC) staff with a holistic network overview
- They should therefore be regarded as a further development of conventional IDS/IPS systems
- The GLACIER project will provide the following features:
  - Unification and consolidation of log information
  - Horizontal scalability
  - Anomaly detection for automated intrusion detection
  - Development of novel multidimensional anomaly detection algorithms
  - Visualization of the anomaly results
- Main issue: Building of an intelligent SIEM system with an open architecture for IT and OT networks

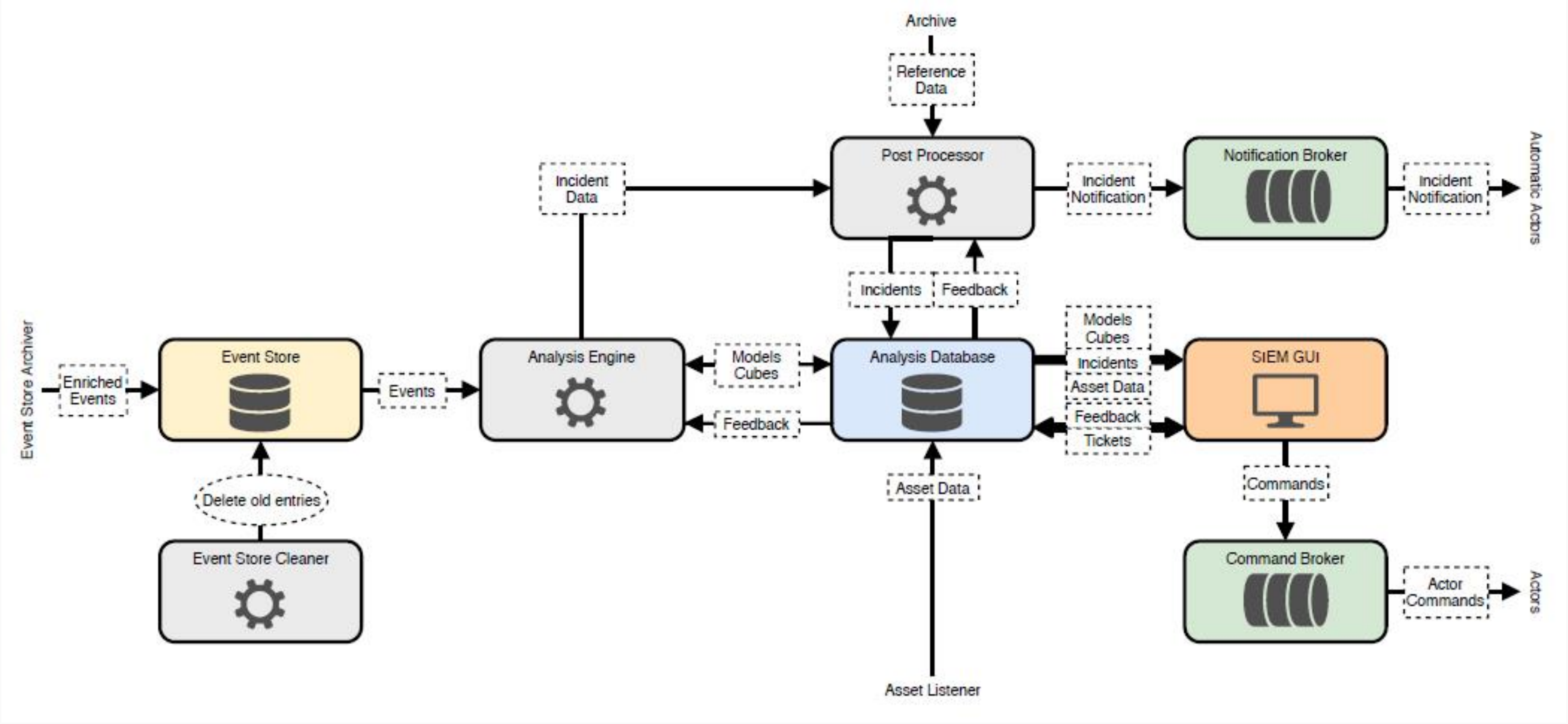
GLACIER architecture

- **Data Collection:** heterogeneous data are gathered from dynamic sources and consolidated as necessary for security analysis.
- **Data Analysis:** Enriched data are forwarded to this component for anomalies detection.
- **Management:** All components are configured and supervised by Management-GUI and administrated by SIEM-GUI.



Data Analysis

- The component responsible for finding anomalies in the event stream, as well as hosting experiments with anomaly detection algorithms, is the Analysis Engine:



Anomaly Detection

- Found anomalies are assigned an anomaly score and an ID, and are treated as incidents in the later parts of data analysis
- The analysis engine utilizes novel machine learning algorithms, which use OLAP cubes as underlying data structure
- Machine learning models, cubed training and inference data and user feedback are stored in the analysis database and retrieved if needed
- This is required especially in the case that the models need to be retrained on updated training data or new feedback
- The Post Processor takes incident data produced by the analysis engine and enriches it for display in the SIEM GUI

Conclusions

- The architecture of GLACIER will provide the required features for security based anomaly detection in IT and OT environments, including wireless networks
- In particular, to improve anomaly detection results, more sensors have to be added to the system to provide further options for describing the normal system state and in consequence analyze potential deviations
- This is useful for both office as well as industrial settings
- The system architecture of GLACIER is a good step forward towards achieving a security incident analysis system which can flexibly adjust to changing system behaviour due to its anomaly detection based approach

Thank you for your attention!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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