SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS

Arne Thiele
HAW Hamburg
27.11.2018
Grundseminar WiSe 2018

Gliederung

- Motivation
- Grundlagen
  - *Intrusion Detection Systems und Infrastruktur*
  - *Event-Korrelation*
  - *Security Operation Center (SOC)*
  - *Computer Security Incident Response Teams (CSIRTs)*
- Beispiel: Ein Open Source System
- Forschung und Konferenzen
- Ausblick

Motivation

- Erkennung von Angriffen oder schädlichem Verhalten
- Vielzahl an Sensoren mit eigenen GUIs
- Erhobene Daten nicht zusammengeführt
- Fehlalarme müssen von Personal bearbeitet werden
- Geschaltete Alarme müssen priorisiert werden

→ Zentraler Punkt für Visualisierung, Analyse und Informationsaggregation benötigt

→ Entlastung des Personals durch Unterstützung in Workflows

GRUNDLAGEN

Grundlagen

- Intrusion Detection Systems (IDS)
  - *Erkennung von schädlichem Verhalten oder Angriffen*
  - *Host-based Intrusion Detection Systems (HIDS)*
  - *Network-based Intrusion Detection Systems (NIDS)*
- Erkennungsmethoden
  - *Fehlverhalten-Erkennung*
    - Regelbasiert: Definiere Fehlverhalten und erkenne anhand dieser Regeln
  - *Anomalie-Erkennung*
    - Modellbasiert: Lerne „normales“ Verhalten und erkenne Abweichungen davon

Grundlagen

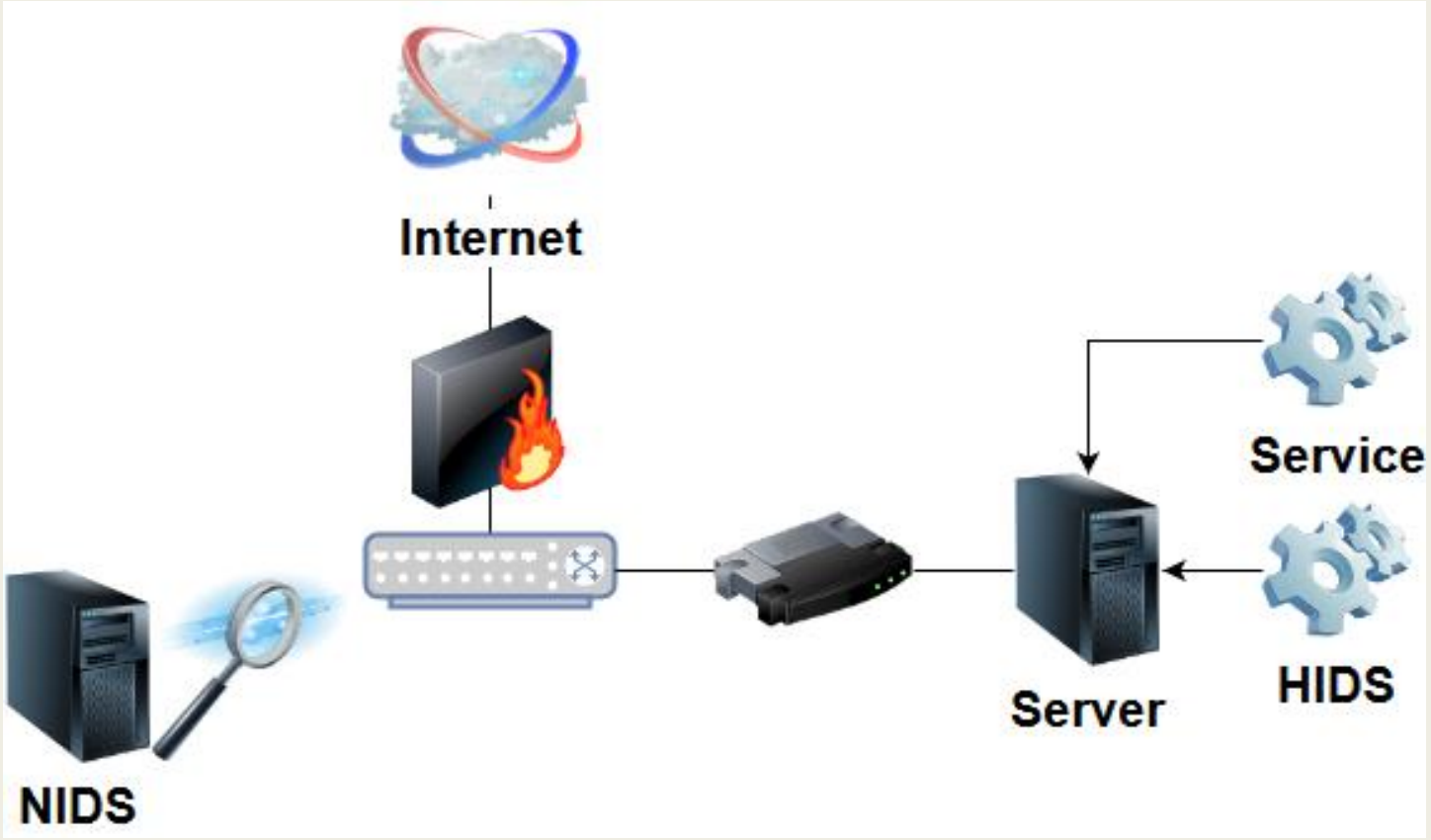


Abbildung 1: *Intrusion Detection Systems in einem Netzwerk*

Grundlagen

- Event-Korrelation

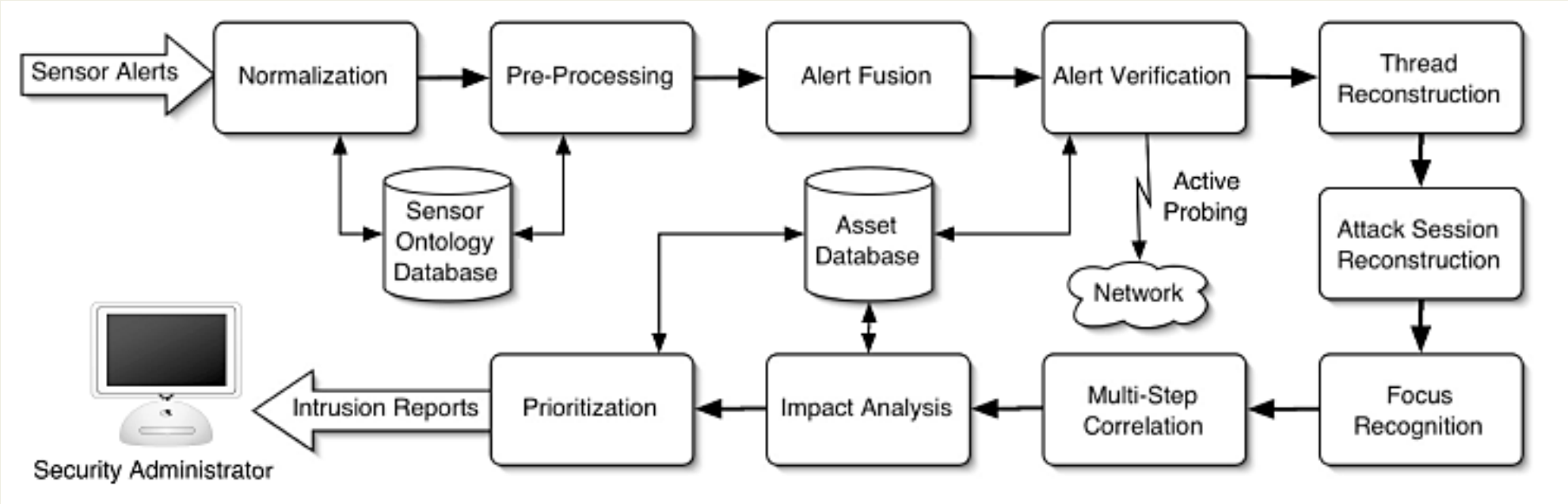


Abbildung 2: Korrelationskomponenten nach Valeur et al [1]

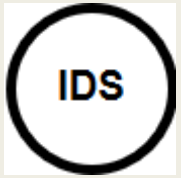
Grundlagen

- Security Operation Center (SOC) [3]
  - *Analysten Level 1:*
    - Entscheidung – Fehlalarm oder potentieller Sicherheitsvorfall?
  - *Analysten Level 2:*
    - Validierung – Genauere Analyse des potentiellen Sicherheitsvorfalls
  - *Security Engineers / SOC-Engineers*
    - Anpassung und Erstellung von funktionalen Komponenten des SOC

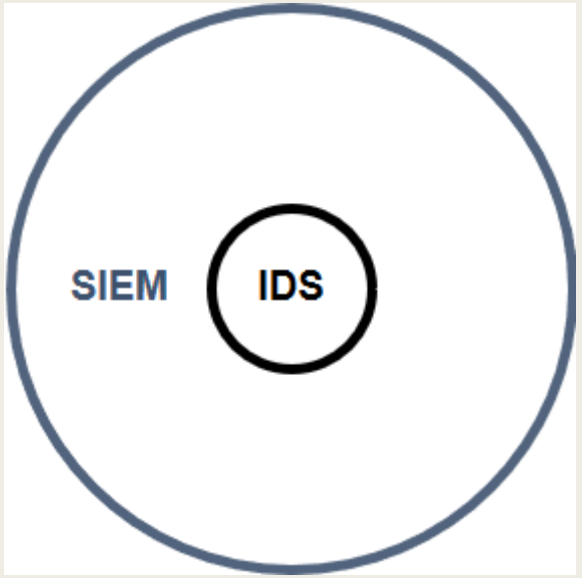
Grundlagen

- Computer Security Incident Response Team (CSIRT) [3]
  - *Team aus erfahrenen Sicherheitsanalysten*
  - *Verbinden SIEM-System mit Threat Intelligence*
  - *Analysieren Sicherheitsvorfälle, dämmen Ausbreitung ein und leiten Gegenmaßnahmen ein*

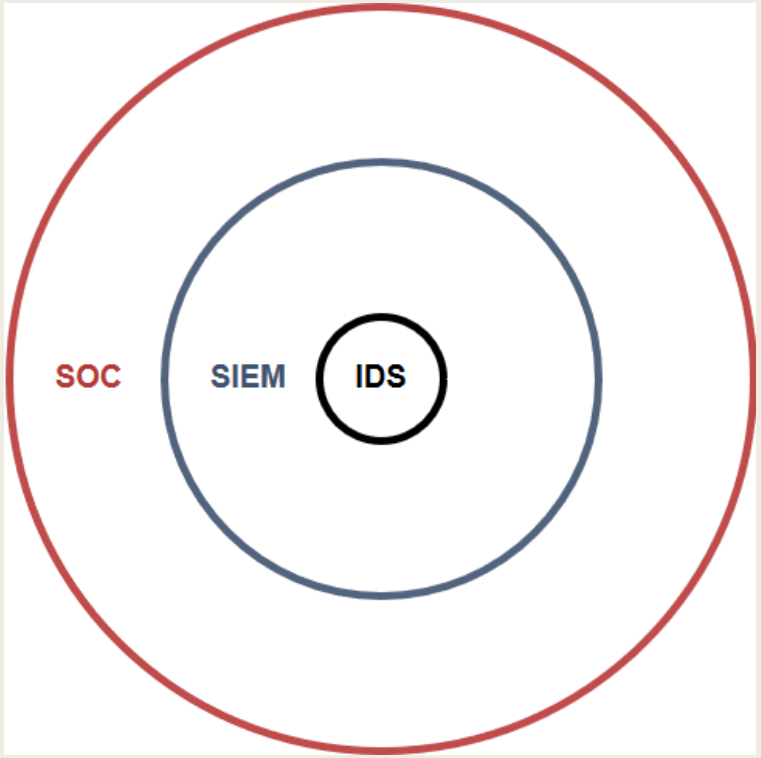
Grundlagen



Grundlagen



Grundlagen



Grundlagen

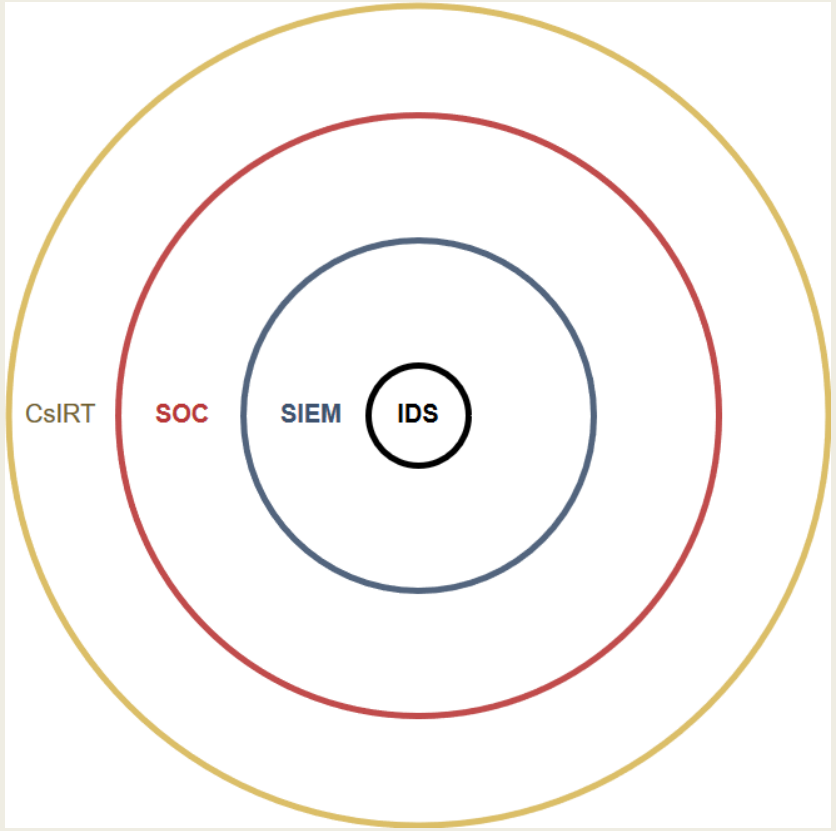


Abbildung 3: Der Intrusion-Detection-Prozess und dessen Bestandteile

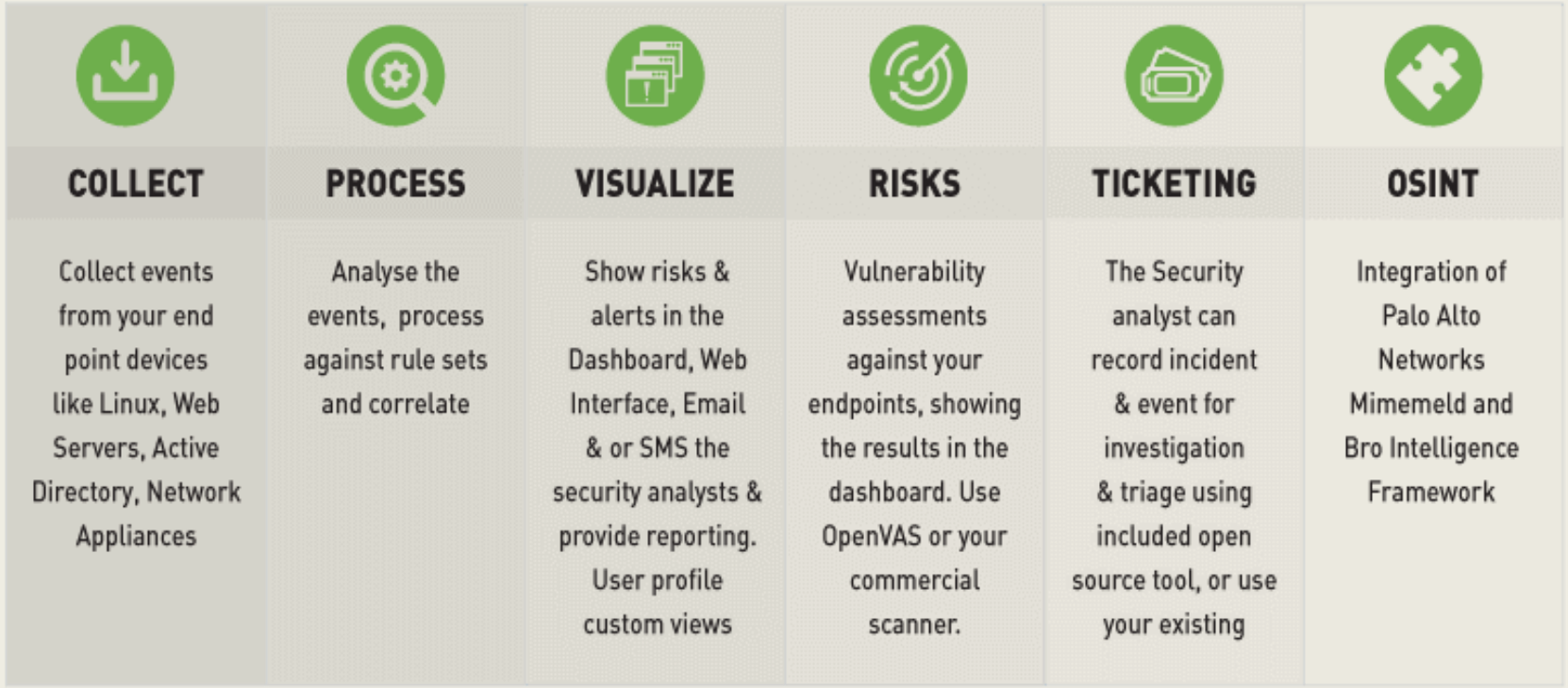
BEISPIEL

SIEMonster - Ein Open Source SIEM-System

SIEMonster Technologie-Stack

Abbildung 4: SIEMonster Tech-Stack nach [2]

Angebotene Features



COLLECT	PROCESS	VISUALIZE	RISKS	TICKETING	OSINT
Collect events from your end point devices like Linux, Web Servers, Active Directory, Network Appliances	Analyse the events, process against rule sets and correlate	Show risks & alerts in the Dashboard, Web Interface, Email & or SMS the security analysts & provide reporting. User profile custom views	Vulnerability assessments against your endpoints, showing the results in the dashboard. Use OpenVAS or your commercial scanner.	The Security analyst can record incident & event for investigation & triage using included open source tool, or use your existing	Integration of Palo Alto Networks Mimemeld and Bro Intelligence Framework

Abbildung 5: Der Dokumentation von SIEMonster entnehmbare Features [2]

Architektur und Datenfluss

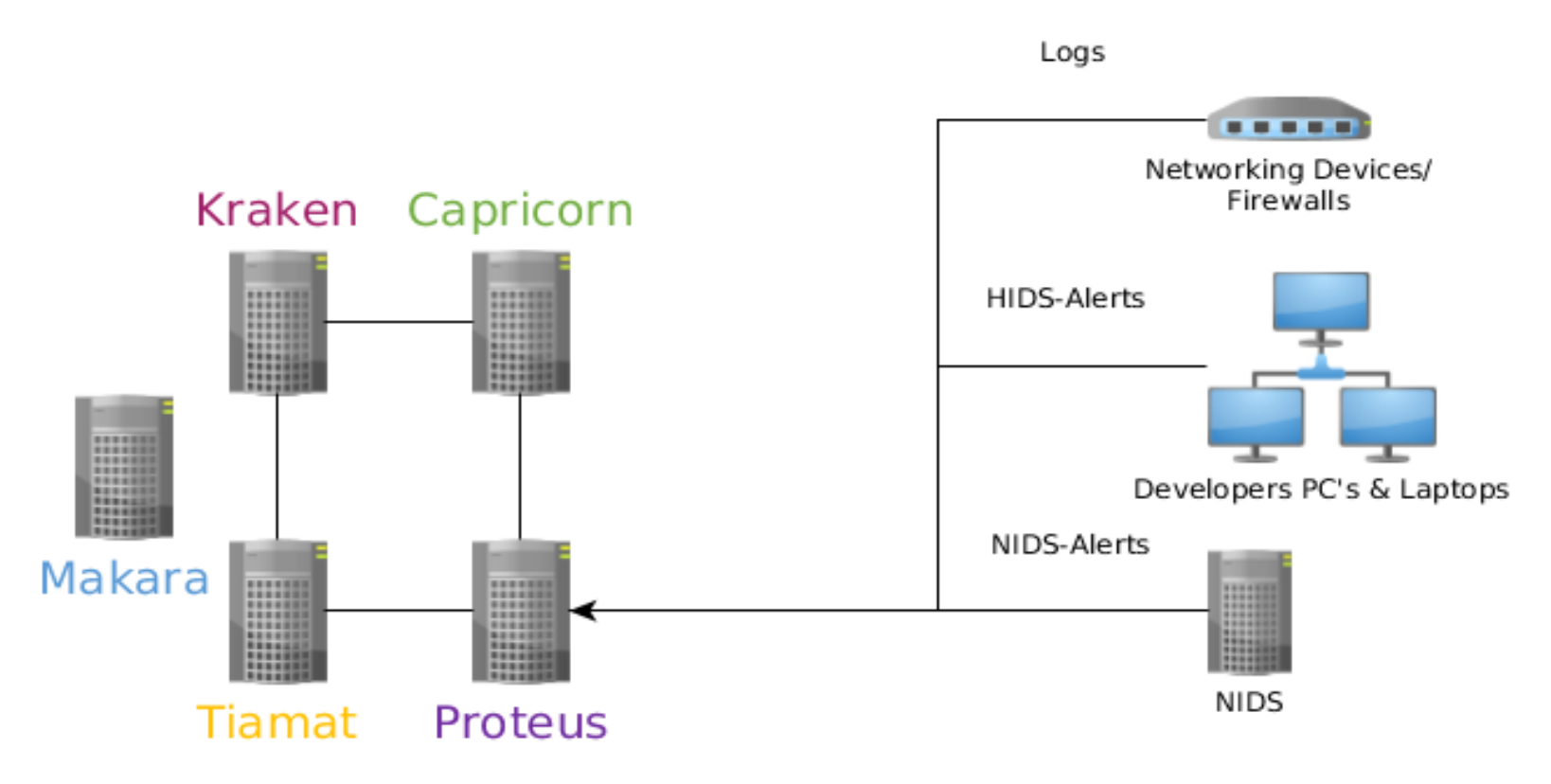


Abbildung 6: SIEMonster Architektur und Datenfluss nach [2]

SIEMonster und Event-Korrelation (?)

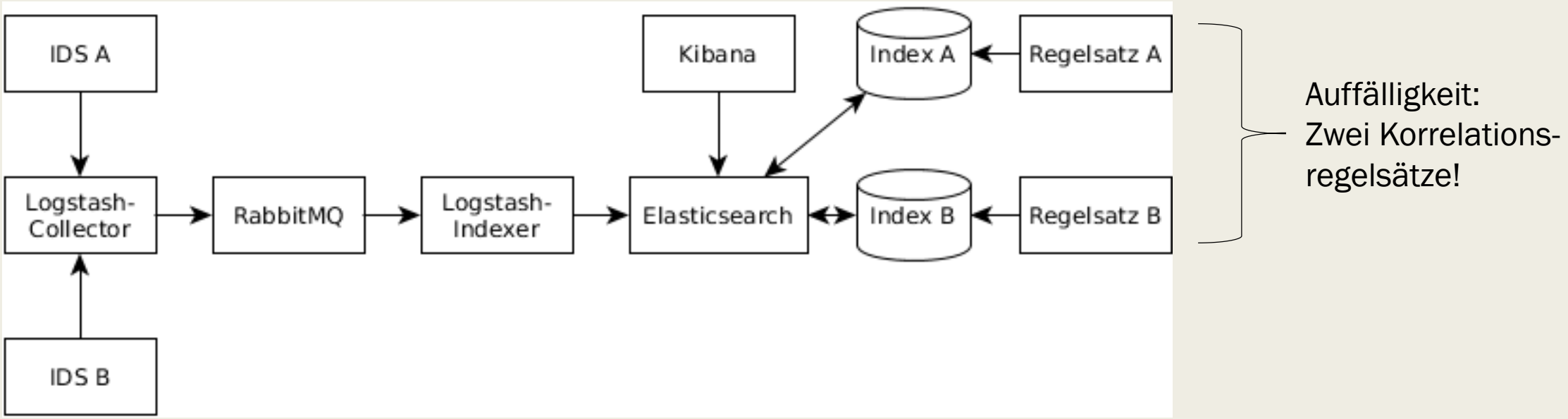
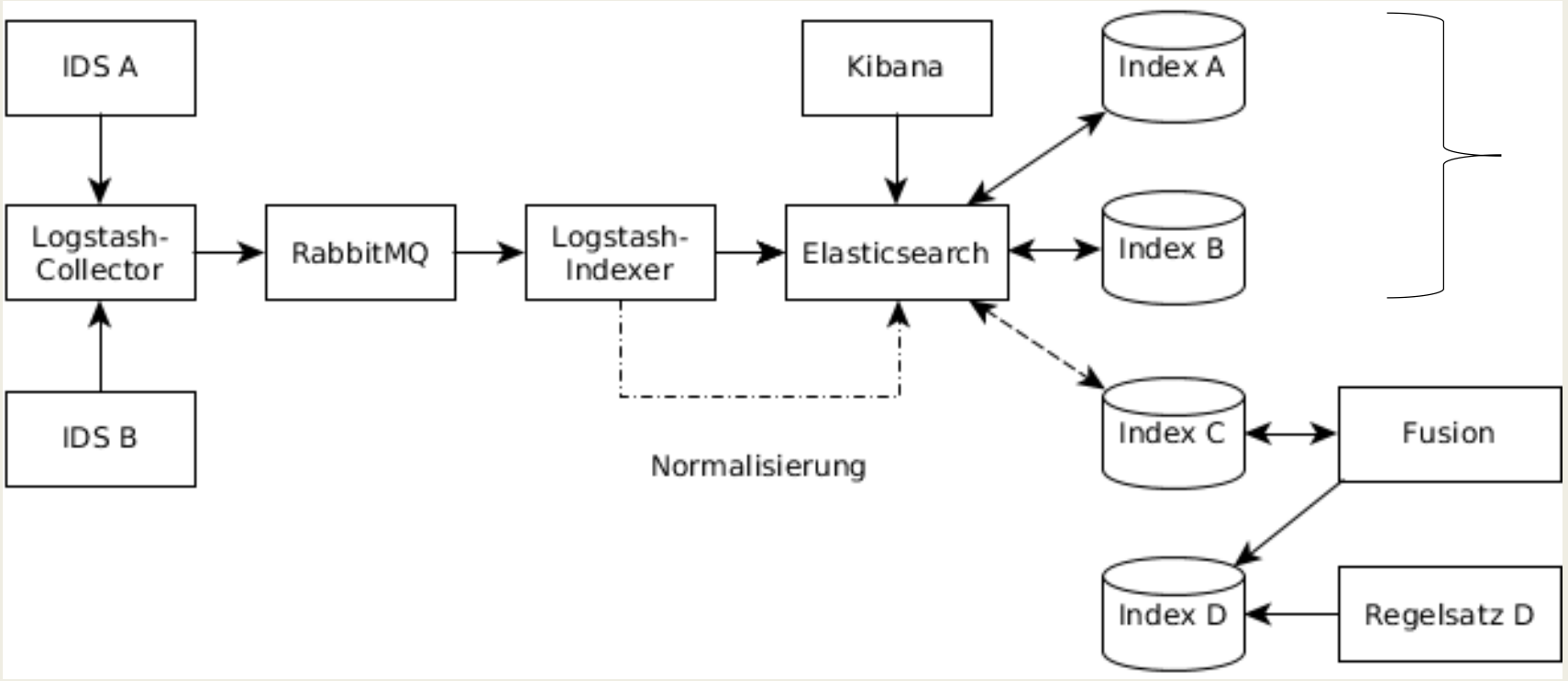


Abbildung 7: Alarmverarbeitung von SIEMonster am Beispiel von zwei IDS

Identifiziertes Problem: Keine übergreifende Korrelationsmöglichkeit

SIEMonster und Event-Korrelation (!)

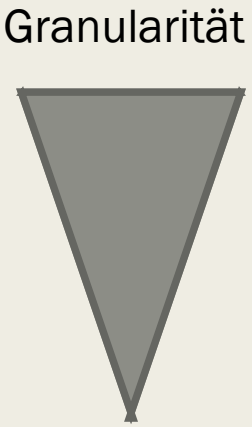


Die bestehenden Regelsätze können erhalten bleiben!

Abbildung 8: Erweiterung des Korrelationsprozesses von SIEMonster

Korrelationsregeln

- Anomalie an einem nicht Werktag → Das Büro müsste eigentlich geschlossen sein
- Priorisierung: Die Risikoeinschätzung des IDS übersteigt einen festen Grenzwert
- Beide IDS entdecken Auffälligkeiten und schalten gleichzeitig einen Alarm
- SSH-Zugriff auf einen Rechner, der dies nicht unterstützen sollte



→ Korrelationsregeln sind stark kontextabhängig und müssen individuell angepasst werden

FORSCHUNG UND KONFERENZEN

Forschung und Konferenzen

- Fragestellungen / Forschungsthemen
  - *Integration von Threat Intelligence*
  - *Verbesserungen der Entscheidungsunterstützung für Personal*
  - *Sinnvolle Verwertung von gespeicherten Daten*

- Konferenzen
  - *Defcon – jährlich, in Amerika*
  - *DFN-Konferenz(en) – jährlich, in Hamburg*
    - IT-Sicherheit in vernetzten Systemen
    - Datenschutz

AUSBLICK

Ausblick

- Erweiterte Auseinandersetzung mit dem Thema Event-Korrelation
- Entwurf eines Open Source Technologie basierten, modularen SIEM-Systems

ZEIT FÜR FRAGEN

Quellen

1. Comprehensive approach to intrusion detection alert correlation; in IEEE Transactions on Dependable and Secure Computing 2004, Vol. 1, number 3, pages 146-169 - F. Valeur, G. Vigna, C. Kruegel and R. A. Kemmerer – URL: https://ieeexplore.ieee.org/document/1366134 (06.06.2018)
2. SIEMonster Version 3 High Level Design; May 2018; Chris Rock and James Bycroft; URL: https://dyzz9obi78pm5.cloudfront.net/app/image/id/5af953a3ad121c9c30841d43/n/siemonster-v3-high-level-design-v15.pdf (26.11.2018)
3. The Operational Role of Security Information and Event Management Systems - Sandeep Bhatt, Pratyusa K. Manadhata und Loai Zomlot; URL: https://ieeexplore.ieee.org/document/6924640 (26.11.2018)
4. The Architecture of a Network Level Intrusion Detection System - Richard Heady, George Luger, Arthur Maccabe and Mark Sevilla
5. Network Intrusion Detection System using attack behavior classification; in: 2014 5th International Conference on Information and Communication Systems (ICICS) - O. Al-Jarrah and A. Arafat
6. Ten Strategies of a World-Class Cybersecurity Operations Center – Carson Zimmerman; ISBN 978-0-692-24310-7
7. DFN-Konferenz https://www.dfn-cert.de/veranstaltungen/CfPSicherheitskonferenz2019.html (25.11.2018.)
8. COUNTERMESASURE Konferenz https://www.countermeasure.ca/ (25.11.2018)
9. DEF CON https://www.defcon.org/index.html (25.11.2018)