Automatisierte Erzeugung von Korrelationsregeln

Unterstützung der Arbeit von Sicherheitsanalysten in einem SOC

Gliederung

- Grundlagen
  - SIEMs
  - Security Event Correlation
  - SOCs und Analysten
  - CERTs
- Rückblick: Grundseminar & -projekt
  - Verarbeitungskette
  - Fusionskomponente
- Erweiterungsmöglichkeiten der Verarbeitungskette
- Korrelationsalgorithmen
  - Similarity-based algorithms
  - Knowledge-based algorithms
  - Statistical-based algorithms
- Ausblick

Grundlagen

Security Information and Event Management (SIEM)

- Datensenke verschiedenster Alarme
- Korrelation zu Meta-Alarmen
- Aufbereitung von Security Incidents
- (Teil-) Automatisierung von reaktiven Mechanismen

Security Event Correlation 1/3

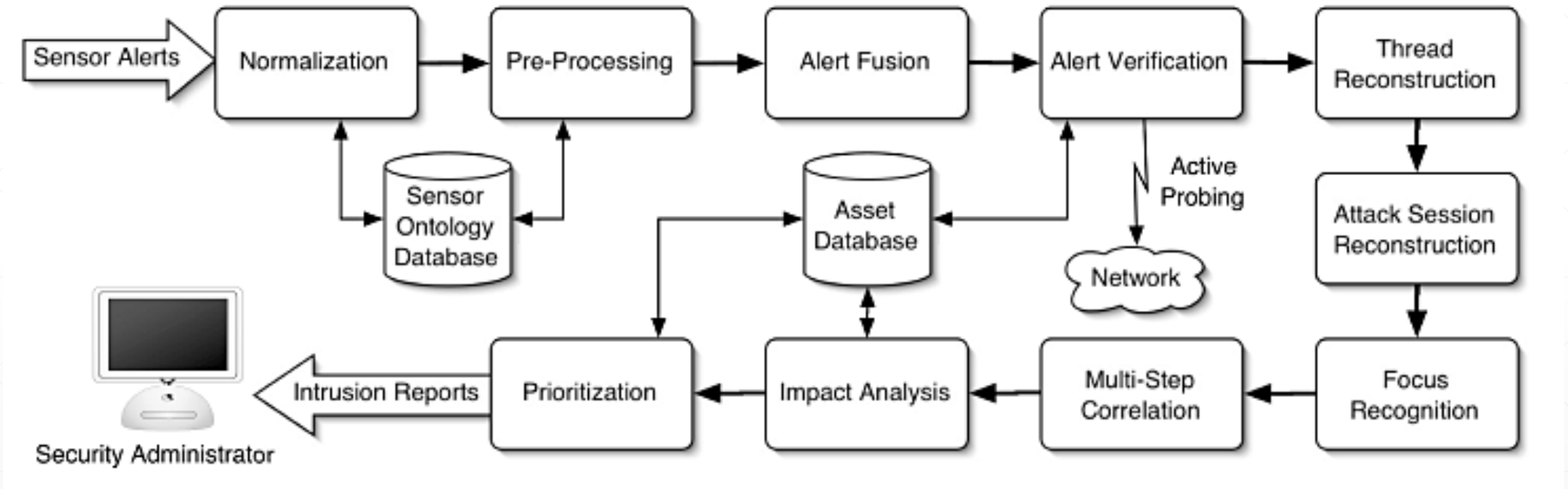

Abbildung 1: Security Event Correlation nach Valeur et. al [1]

Security Event Correlation 2/3

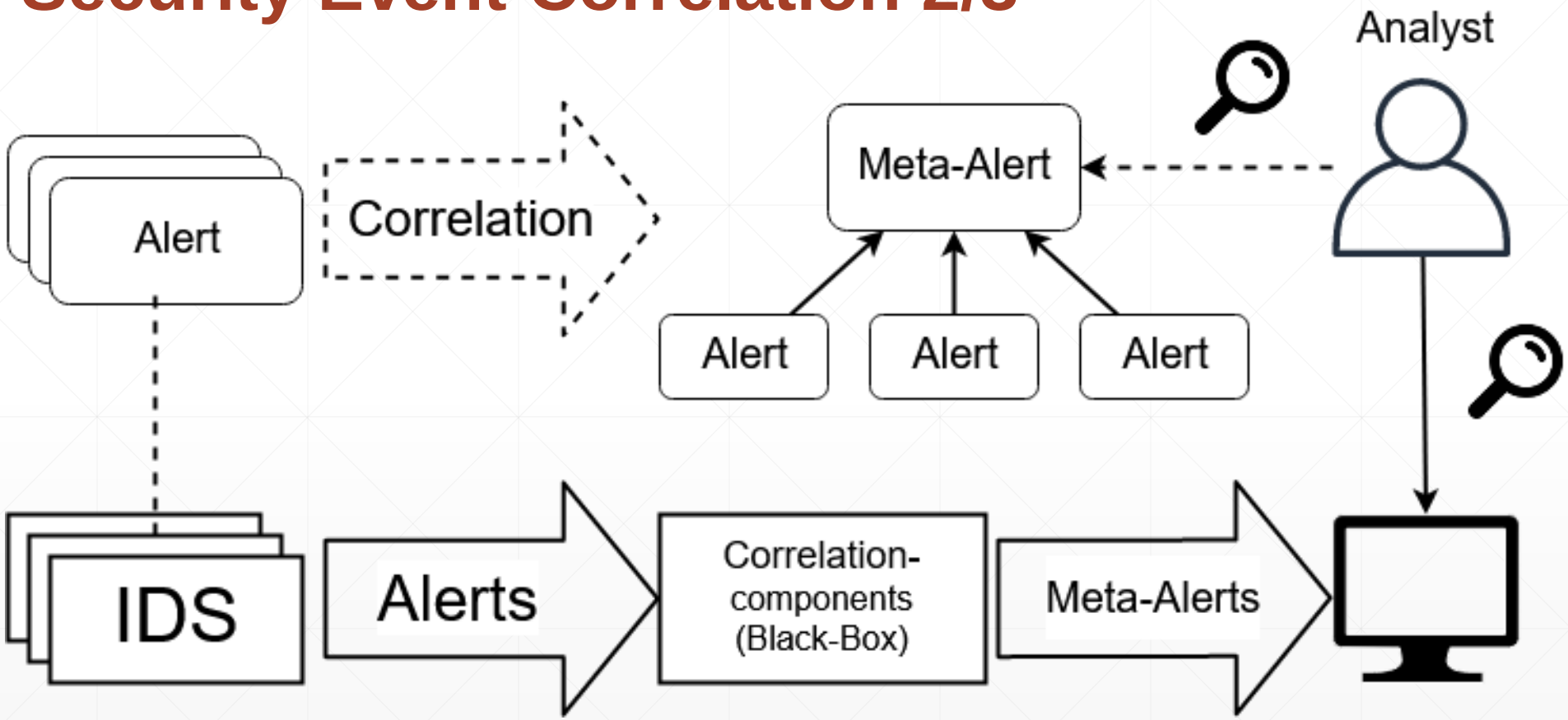

Abbildung 2: Grundlegende Alarm-Korrelation und Datenstruktur

Security Event Correlation 3/3

- Ziele
  - Reduzierung der Fehlalarme
  - Reduzierung der zu untersuchenden Alarme
  - Aufbereitung der erkannten Vorfälle

Security Operations Center (SOC)

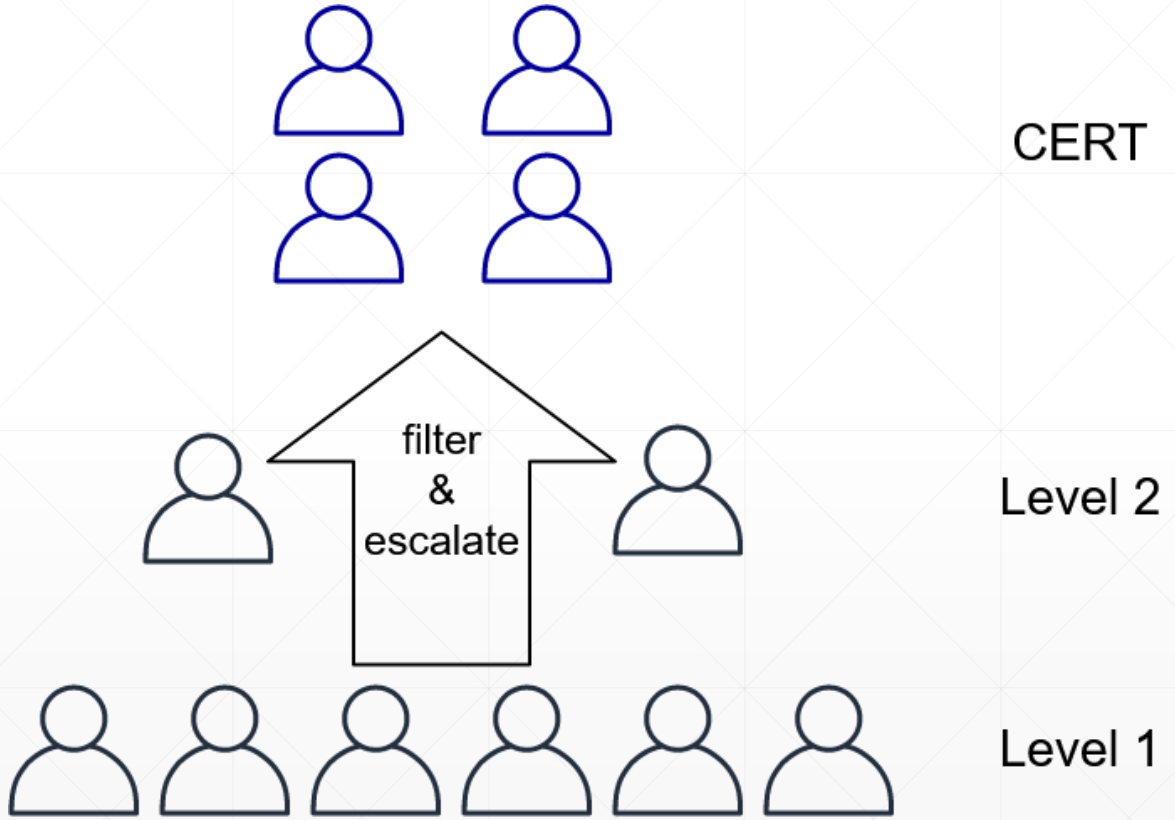

Abbildung 3: Hierarchische Anordnung von Analysten in einem SOC [4]

Security Operations Center (SOC)

- Hierarchische Anordnung von Analysten um ein (oder mehrere) SIEMs
- Zugehörig zu bestimmter Infrastruktur (Rechenzentrum etc.)
- Sortierung und Investigation von Meta-Alarmen
- Priorisierung und ggf. Eskalation eines Incidents an CERT

Computer Emergency Response Team (CERT)

- CERT ist geschützter Begriff, daher oft auch Computer Security Incident Response Team (CSIRT)
- Team aus erfahrenen Analysten
- Eindämmung von Security Incidents

→ Reaktives Team

Rückblick: Grundseminar & -projekt

Verarbeitungskette

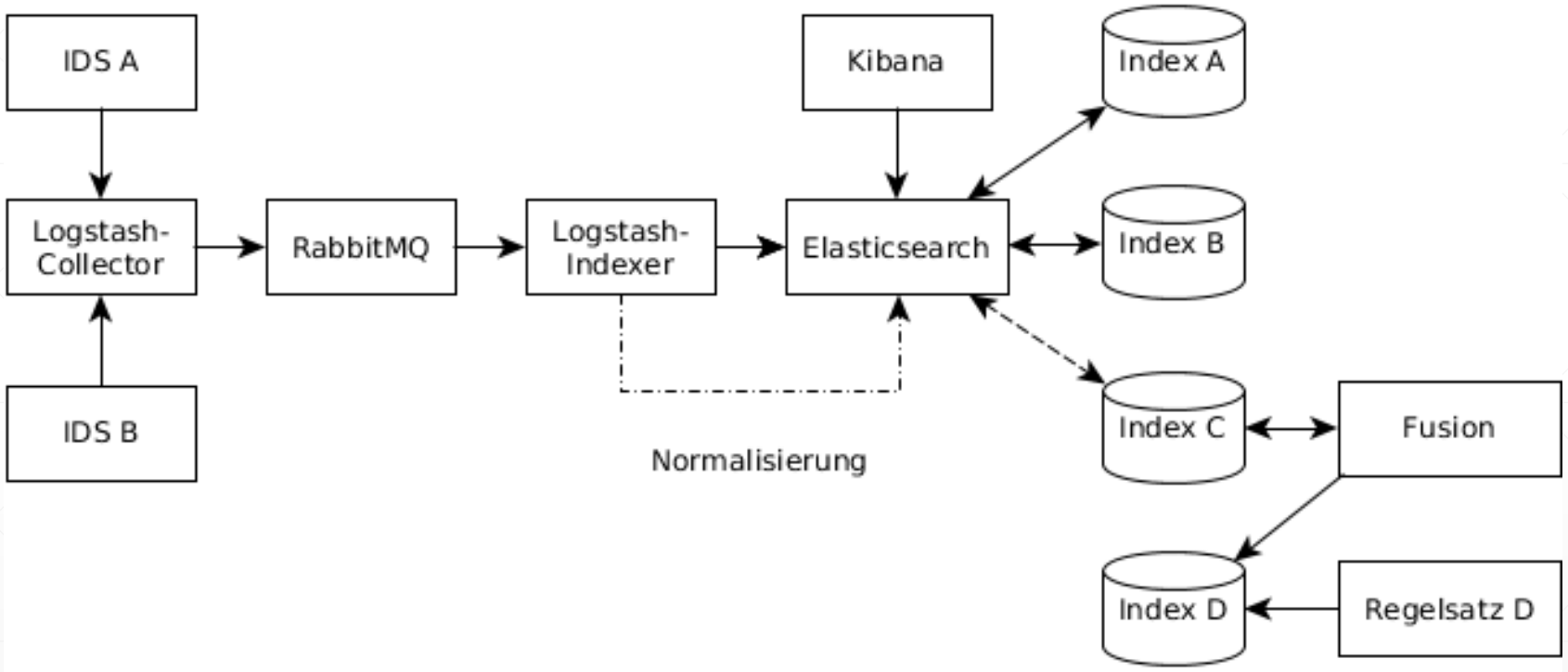

Abbildung 2: Verarbeitungskette aus dem Grundseminar

Fusionskomponente

- Finde heraus welche Alarme von der gleichen Aktion ausgelöst wurden
- Fasse wenn möglich die Alarme zu einem Meta-Alarm zusammen
  - Setzt Normalisierung voraus (bspw. Intrusion Detection Message Exchange Format [5])
  - Setzt Umgang mit nicht gesetzten Alarmwerten voraus

  → Dreiwertige Logik

Erweiterungsmöglichkeiten der Verarbeitungskette

Erweiterungsmöglichkeiten

- Regelerzeugungskomponente
- Simulationskomponente
- Vorschlagskomponente (UI für Analysten)

Regelerzeugungskomponente

- Erzeugt neue Regeln und fügt sie altem Regelsatz hinzu
- Soll Fein-Tuning von bestehenden Regeln teilautomatisiert unterstützen

Simulationskomponente

- Spielt verschiedene Regelsätze durch und vergleicht die Ergebnisse
- Benötigt Wissen über Verteilung von Alarmen und Fehlalarmen
- Könnte dazu dienen die tatsächlichen Auswirkungen von neuen Regeln zu verdeutlichen

Vorschlagskomponente (UI für Analysten)

- Führt Simulations- und Regelerzeugungskomponente zusammen
- Analyst kann von Regelerzeugungskomponente entnommene Vorschläge für bestimmten Zeitraum simulieren
- Visualisierung unterstützt den Analysten bei Einführung neuer Regeln

Erweiterungsmöglichkeiten - Fazit

- → Problem: Einzelne Komponenten im Use-Case schwer von einander zu trennen
- → Zu aufwändig um sie gemeinsam in das Hauptprojekt einzugliedern
- → Fokussierung auf automatisierte Regelerzeugung

Korrelationsalgorithmen

Korrelationsalgorithmen nach [2]

- **Similarity-based algorithms**
  - Simple Rules
  - Hierachical Rules
  - Machine Learning
- **Knowledge-based algorithms**
  - Prerequisites/Consequences
  - Scenario
- **Statistical-based algorithms**
  - Statistical Traffic Estimation
  - Causal Relation Estimation
  - Reliability Degree Combination

Zusätzliche Quellen: [6],[7] und [8]

Similarity-based algorithms

Vorteile

- ✓ Einzelne Regeln sind leicht zu schreiben
- ✓ Gute Parallelisierbarkeit der einzelnen Regeln
- ✓ Absehbarer Speicherbedarf
- ✓ Bietet Möglichkeiten für Machine Learning (Clustering)

Nachteile

- – Closed-World-Assumption
- – Training von ML-Ansätzen benötigen gut aufbereitete Datensätze

Knowledge-based algorithms

Vorteile

- ✓ Erweiterung der Wissensbasis gewährleistet hohe Flexibilität
- ✓ Sehr präzise Analysemöglichkeiten
- ✓ Graphen-Strukturen lassen ggf. Optimierungen zu
- ✓ Einzelne Schritte der Szenarios gut nachvollziehbar

Nachteile

- – Closed-World-Assumption
- – Benötigen viel Rechenkapazität

Statistical-based algorithms

Vorteile

- ✓ Kein Hintergrundwissen notwendig
- ✓ Durch Möglichkeit von online Justierungen sehr flexibel
- ✓ Attack-Pattern Erkennung integrierbar
- ✓ Können False-Positive Erkennung realisieren

Nachteile

- – Closed-World-Assumption
- – Statistiken liefern immer nur Approximationen
- – Benötigen viele Daten um ein präzises Modell zu erstellen

Ausblick

Ausblick

- Implementierung und Messung eines oder mehrerer Korrelationsalgorithmen
  - Integration in die im GPJ umgesetzte Infrastruktur
  - Messungen unter möglichst realen Bedingungen → Kontakt: Prof. Dr. Kossakowski
- Alle angeschnittenen Komponenten realisieren im Zuge der Masterarbeit
  - (ggf. zu viel Aufwand → Neu-Priorisierung)

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 (13.12.2019)

[2] Alert Correlation Algorithms: A Survey and Taxonomy, January 2013 - Seyed Ali Mirheidari, Sajjad Arshad, Rasool Jalili - Conference: Symposium on Cyberspace Safety and Security (CSS)

[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 (13.12.2019)

[4] Intrusion Detection Effektiv! Modellierung und Analyse von Angriffsmustern - Dr. Michael Meier 2007,
ISSN 1611-8618, ISBN-13 978-3-540-48251-2

Quellen(2)

[5] H. Debar, D. Curry, B. Feinstein, "The intrusion detection message exchange format (IDMEF). RFC4765", *Network Working Group*, 2007.

[6] Valdes, A., Skinner, K.: Probabilistic alert correlation. In: Recent Advances in Intrusion Detection (RAID), pp. 54-68 (2001)

[7] Ning, P., Cui, Y., Reeves, D. S., Xu, D.: Techniques and tools for analyzing intrusion alerts. In: ACM Transactions on Information and System Security (TISSEC), vol. 7, no. 2, pp. 274-318 (2004)

[8] Lee, W., Qin, X.: Statistical causality Analysis of INFOSEC alert data. In: Managing Cyber Threats.,pp. 101-127 (2003)

Zeit für Fragen