Hochschule Worms

Fachbereich Informatik

Studiengang Angewandte Informatik B.Sc.

TBD

Bacherloarbeit xxx

Bruno Macedo da Silva
676839
inf3645@hs-worms.de
Bebelstraße 22 Z10
67549 Worms

Betreuer	Prof. Dr. Zdravko Bozakov
Bearbeitungszeitraum:	Sommersemester 2023
Abgabedatum:	xx. xxx 2023
Sperrvermerk:	Ja/Nein

Inhaltsverzeichnis

Abstract

XXXXXXXXXXXXXXXXXXX

Abbildungsverzeichnis

Glossar

Künstliche Intelligenz (KI) Der Konzept, dass Maschine kognitive menschliche Fähigkeit entwickeln können, wie Verständnis, Entscheitungstreffen, Lernen, Problemlösung und (Collins et al., 2021).

National Institute of Standards and Technology (NIST) US-Behörden, die für die Reglungen, Vereinheitlichung und Weiterentwicklung im Bereich Informationstechnologie zuständig ist (Hochschule Worms, 2018) .

Cyberangriff Angriffe, die über den Cyberspace stattfinden. Solche Angriffe zielen auf Unternehmen und deren Infrastrukturen, um sie zu zerstören, lähmen, kontrollieren oder die Integrität deren Daten zu stehlen oder zu dominieren (NIST, 2020a).

Open Source beschreibt Code, die jeder zugreifen, modifiziren und verbreiten können, ohne dafür Lizenzen bezahlen zu müssen (Open Source Initiative, 2007).

Proprietary bezieht sich auf Software, die einer Firma oder Person gehören. Für die Nutzung ist meisten den Kauf einer Lizenz notwendig. In diesem Fall haben den Kunden wenig oder kaum Zugang zu den originillen Code(Nexcess, 2022).

Abkürzungsverzeichnis

CIA Confidentiality, Integrity and Availability.

FPO Fachspezifische Prüfungsordnung.

KI Künstliche Intelligenz.

NIST National Institute of Standards and Technology.

SEM Security Event Management.

SIEM Security Information and Event Management.

SIM Security Information Management.

1 Einleitung

Der heutige Netzwerkverkehr ist fast tausendfach größer als vor 20 Jahre (Roser et al., 2015). Das Internet wird heutzutage für fast alle unsere alltägliche Tätigkeit verwendet: Sozialenetzwerke, Video und Audio-Streaming, Einkauf, behördliche Angelegenheit und viele andere. So viel Verkehr generiert eine unermessliche Menge von Daten, die alle mögliche Inhalte beinhalten, von unschuldigen Anfragen nach dem eigenen Kontostand bis zu der Ausführung von bösewichten Anfragen, um Systemen lahmzumachen. Um das erste von der zweiten zu Unterscheiden verwenden vielen Firmen die sogennanten Security Information and Event Management (SIEM).

Die National Institute of Standards and Technology (NIST) definiert als Anwendung, die dafür zuständig ist, Sicherheitsdaten von anderen Systemen zu sammeln und diese verständlich und lesbar als Information zu liefern. Mit diesem Ergebnis können Aktionen und durchgeführt werden können (NIST, 2020b). Die Bewertung dieser Daten spielt eine wesentliche Rolle bei solchen Anwendungen, da es entscheidend ist, ob es um eine oder viele normale Anfrage oder um einen Cyberangriff geht.

In diesem Projekt wollen wir über eine existierende Open Source SIEM-Anwendung recherchieren und ihre Extrahierung und Bewertung von Daten analysieren, sodass wir schließlich eine einige Lösung für die Identifizierung von spezifische Cyberangriffe entwerfen können.

Diese Arbeit wird in folgende Teile geteilt:

- Beschreibung von existierenden SIEMs see und Vergleich zwischen privaten Anbieter und eine Open Source Lösungen (Alienvault OSSIN, OpenSearch, MozDef, Wazuh, Preludes)
- Analyse der Funktionalität einer Open Source SIEM
- Definition von zwei spezifische Cyberangriffe
- Empfang und Bearbeitung der Daten von den vorher beschriebenen Angriffe
- Entwicklung einer Regel für die Erkennung eines Cyberangriff

- Analyse und Bewertung der Arbeit

1.1 Problemstellung

Während der Entwicklung dieser Arbeit wollen wir uns mit folgenden Fragen beschäftigen:

- Welche Information-Muster muss von dem SIEM extrahiert werden, um Angriff_1 und Angriff_2 zu erkennen?
- Wie sollen aussagenkräftige Use-Cases / Regel sein, um Angriff_2 und Angriff_2 richtig zu erkennen zu erkennen?
- Wie sollen Server-Logs aussehen, damit sie von SIEMs see bearbeiten werden können.
- Was bringt Künstliche Intelligenz (KI) zu der Zukunft von SIEMs see ?

Note: Für Angriffe habe ich an DoS und Brute-Force (Password Spraying/Dictionary) gedacht.

Note 2: Punkt 3 wäre eher theoretisch, um zu recherchieren, was es schon gibt und was schon darüber geschrieben wurde.

1.2 Vorgehensweise

Um diese obengenannten Ziele zu erreichen, verwenden wir folgenden Methode:

- Installation von virtuellen Maschinen zur Nutzung von der ausgewählten SIEM und zur Generierung von Server-Logs
- Nutzung von Container zur Installation von SIEM

2 Definition von SIEN

SIEM ist das Ergebnis von der Kombination zwischen Security Event Management (SEM) und Security Information Management (SIM) (Dorigo, 2012). Das erste bezieht sich auf der Identifizierung, Bewertung, Beobachtung und Bericht von Sicherheitsvorfällen mithilfe von verschiedenen Logdateien (techopedia, 2015). Das zweite ist ein Software, der bei der automatischen Sammlung von Loginformationen aus vielen Quellen, wie Firewall und Servers, untersützt techopedia (2022).

https://community.microfocus.com/cyberres/b/sws-22/posts/sim-sem-and-siem-definitions-and-choosing-the-right-enterprise-solution

Um diese obengenannten Ziele zu erreichen, verwenden wir folgenden Methode:

- Was ist SIEN in der Literatur?
- State of Art the Art
- kurzer Vergleich zwsichen *Proprietary* und Open Source Lösungen
- Existierende Rechecher über das Thema

- Architektur

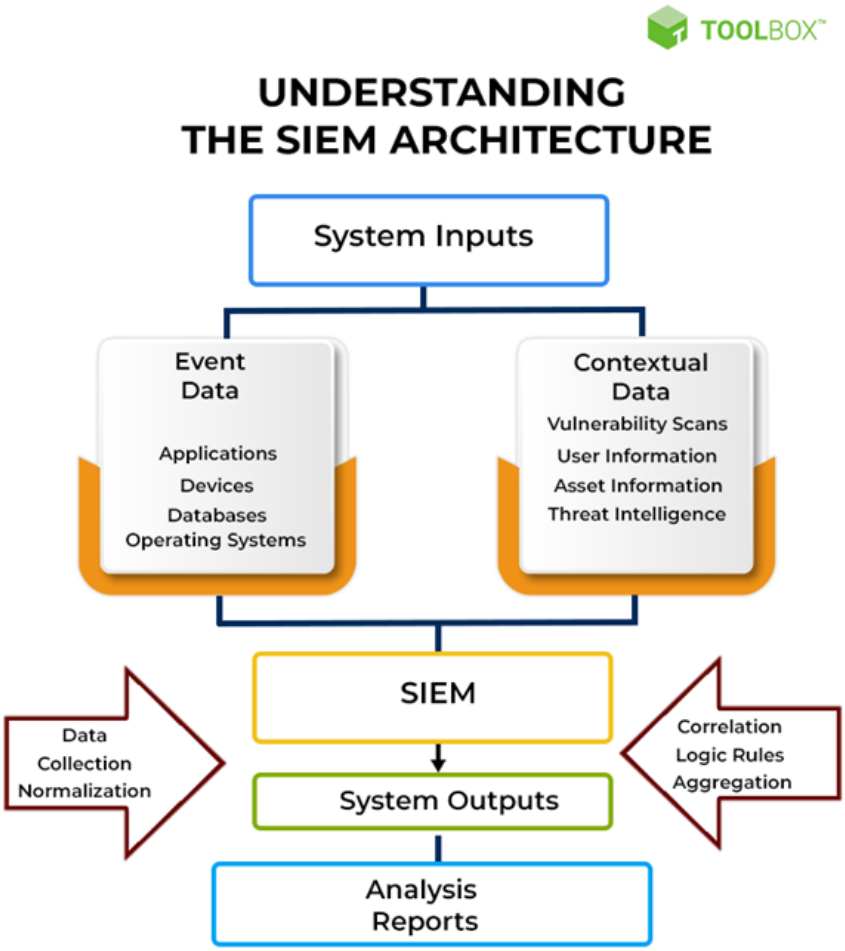

Abbildung 1: Allgemeine Informationsfluss von SIEM
Quelle: (Mohanan, 2022)

- Anpassung

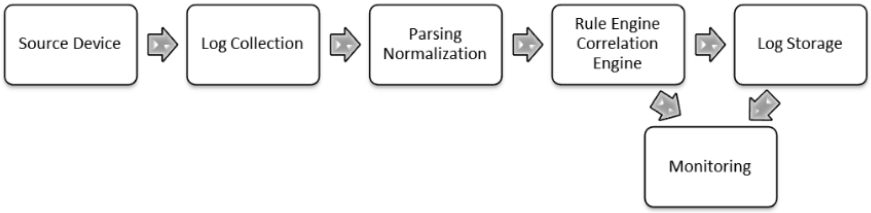

Abbildung 2: Allgemeine Informationsfluss von SIEM
Quelle: (Granadillo et al., 2021)

3 Implementation

3.1 Installation von SIEM in Container

Hier werden die Schritte für die Installation und Sammeln von Daten beschrieben.

- Implementation in Container

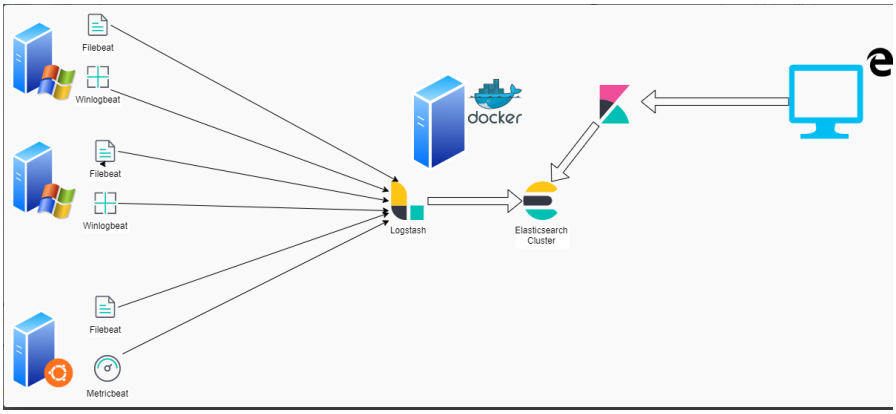

Abbildung 3: Struktur von SIEM in einem Container
Quelle: (RDR_IT, 2022)

3.2 Sammlung von Server-Log Dateien

3.3 Normalisierung der Log-Dateien

4 Fazit

Zuammenfassung von

- Zielen
- Ergenissen
- Herausforderungen

4.1 Zukünftige Entwicklungen

Literaturverzeichnis

Collins, C., Dennehy, D., Conboy, K., and Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*, 60:102383. https://www.sciencedirect.com/science/article/pii/S0268401221000761. Zugriff am 21.2.2023.

Dorigo, S. (2012). Security Information and Event Management. Master's thesis, Radboud University Nijmegen. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiNu-XkhsD9AhV4FzQIHdMkBWYQFnoECCYQAQ&url=https%3A%2F%2Fwww.ru.nl%2Fpublish%2Fpages%2F769526%2Fthesissanderdorigo.pdf&usg=AOvVaw3oPn4KBFwgJwexoXZ1Be40. Zugriff am 3.3.2023.

Granadillo, G., González-Zarzosa, S., and Diaz, R. (2021). Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21:4759. file:///C:/Users/bruno/Downloads/Security_Information_and_Event_Management_SIEM_Ana.pdf. Zugriff am 21.2.2023.

Hochschule Worms (2018). Fachspezifische prüfungsordnung (fpo 2018). https://www.hs-worms.de/fileadmin/media/fachbereiche/informatik/AInf/Pruefungsordnung/AnInf_FPO_2017-12-19_FINAL.pdf. Zugriff am 11.2.2022.

Laue, T., Kleiner, C., and Kai-Oliver Detken, a. T. K. (2021). A siem architecture for multidimensional anomaly detection. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 1, pages 136–142. https://doi.org/10.1109/IDAACS53288.2021.9660903. Zugriff am 20.2.2023.

Mohanan, R. (2022). What is security information and event management (siem)? definition, architecture, operational process, and best practices. https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/. Zugriff am 26.2.2022.

Nexcess (2022). Open source vs. proprietary: Which is better? https://www.nexcess.net/blog/open-source-vs-proprietary/. Zugriff am 26.2.2022.

NIST (2020a). Cyber attacke. https://csrc.nist.gov/glossary/term/Cyber_Attack. Zugriff am 19.2.2022.

NIST (2020b). Cyber attacke. https://csrc.nist.gov/glossary/term/security_information_and_event_management_tool. Zugriff am 17.02.2023.

Open Source Initiative (2007). The Open Source Definition (Annotated). https://opensource.org/definition/. Zugriff am 17.02.2023.

RDR_IT (2022). Elk installation et configuration d'un siem avec docker.

https://rdr-it.com/elk-installation-configuration-un-siem-docker/. Zugriff am 26.02.2023.

Roser, M., Ritchie, H., and Ortiz-Ospina, E. (2015). Internet. *Our World in Data*. https://ourworldindata.org/internet. Zugriff am 17.2.2023.

Tanembaum, A. S. (2009). *Moderne Betriebssysteme*. Pearson, München.

Tanembaum, A. S. and Wetherall, D. (2011). *Computer Networks*. Prentice Hall, München, 5 edition.

techopedia (2015). Security Event Management. https://www.techopedia.com/definition/25763/security-event-management. Zugriff am 03.03.2023.

techopedia (2022). Security Information Management (SIM). https://www.techopedia.com/definition/25763/security-event-management. Zugriff am 03.03.2023.

Wendzel, S. (2018). *IT-Sicherheit für TCP/IP- und IoT-Netzwerke*. Springer Vieweg, Wiesbaden.

Wendzel, S. and Plötner, J. (2007). *Praxisbuch Netzwerk-Sicherheit: Risikoanalyse, Methoden und Umsetzung; für Unix-Linux und Windows; VPN, WLAN, Intrusion Detection, Disaster Recovery, Kryptologie*. Galileo Computing, Bonn.