

**Hochschule Worms**  
**Fachbereich Informatik**  
**Studiengang Angewandte Informatik B.Sc.**

**TBD**

Bachelorarbeit 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

<b>Abstract</b>	<b>3</b>
<b>Abbildungsverzeichnis</b>	<b>4</b>
<b>Glossar</b>	<b>5</b>
<b>Abkürzungsverzeichnis</b>	<b>7</b>
<b>1 Einleitung</b>	<b>8</b>
1.1 Problemstellung . . . . .	9
1.2 Vorgehensweise . . . . .	10
<b>2 Definition von SIEM</b>	<b>11</b>
2.1 Existierende SIEM Lösungen . . . . .	13
2.1.1 Prelude . . . . .	14
2.1.2 AlienVault OSSIM . . . . .	14
2.1.3 ELK Stack . . . . .	15
2.1.4 Zusammenfassender Vergleich . . . . .	15
2.2 Existierende SIEM Lösungen . . . . .	15
<b>3 Implementation</b>	<b>16</b>
3.1 Installation von SIEM in Container . . . . .	16
3.2 Sammlung von Server-Log Dateien . . . . .	16
3.3 Normalisierung der Log-Dateien . . . . .	16
<b>4 Fazit</b>	<b>17</b>
4.1 Zukünftige Entwicklungen . . . . .	17
<b>Literaturverzeichnis</b>	<b>18</b>

## Abstract

XXXXXXXXXXXXXXXXXXXX

## Abbildungsverzeichnis

1	Aufbau dieser wissenschaftlichen Recherche Security Information and Event Management (SIEM) Quelle: Eigene Darstellung . . . . .	9
2	Allgemeine Informationsfluss von SIEM Quelle: (Mohan, 2022) . . . . .	12
3	Allgemeine Informationsfluss von SIEM Quelle: (Granadillo et al., 2021) .	13
4	Struktur von SIEM in einem Container Quelle: (RDR_IT, 2022) . . . . .	16

## Glossar

**Confidentiality, Integrity and Availability (CIA)** Beschreibt die drei wichtigsten Schutzziele der IT-Sicherheit: Vertraulichkeit, Integrität und Verfügbarkeit (Wendzel, 2018).

**Health Insurance Portability and Accountability Act (HIPAA)** US-Bundesgesetz über den Schutz von sensiblen personenbezogenen Gesundheitsdaten (U.S. Department of Health & Human Services, 2016) .

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

**Payment Card Industry Data Security Standard (PCDI DSS)** Sicherheitsstandards, die Unternehmen, die Kreditkarte akzeptieren, bearbeiten, speichern oder übertragen, anwenden müssen (Centers for Disease Control and Prevention, 2016) .

**Security Operations Center (SOC)** zentralisierter Bereich eines Unternehmens dafür zuständig, Sicherheitsvorfälle zu überwachen, zu identifizieren, zu bewerten und dazu zu reagieren (Vielberth, 2021) .

**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).

**falsch positiv** Eine aus einer fehlerhaften erkannten Verwundbarkeit Warnmeldung (NIST, 2020c).

**Open Source** beschreibt Code, die jeder zugreifen, modifizieren 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 meistens der Kauf einer Lizenz notwendig. In diesem Fall haben den Kunden wenig oder kaum Zugang zu den originellen Code (Nexcess, 2022).

**Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2)**  
im Jahr 2021 verabschiedetes Bundesgesetz zur Erhöhung von Sicherheit Informationstechnische Systemen besonders solchen von den kritischen Infrastrukturen (Harmes, 2023).

## **Abkürzungsverzeichnis**

**CIA** Confidentiality, Integrity and Availability.

**FPO** Fachspezifische Prüfungsordnung.

**HIPAA** Health Insurance Portability and Accountability Act.

**IDS** Intrusion Detection System .

**IPS** Intrusion Prevention System .

**KI** Künstliche Intelligenz.

**NIST** National Institute of Standards and Technology.

**OTX** Open Threat Exchange.

**PCDI DSS** Payment Card Industry Data Security Standard.

**SEM** Security Event Management.

**SIEM** Security Information and Event Management.

**SIM** Security Information Management.

**SOC** Security Operations Center.

# 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 bösewichtigen Anfragen, um Systemen lahmzumachen. Um das erste von der zweiten zu Unterscheiden verwenden vielen Firmen die sogenannten 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. Am Ende wollen wir uns für eine der gefundenen Lösung entscheiden, sodass spezifische Logdateien der Hochschule Worms bewertet und bearbeitet werden können.

Diese Arbeit wird in folgende Teile geteilt:

- Beschreibung von existierenden SIEMs 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

Das folgende Diagramm stellt den Aufbau dieser Arbeit dar:

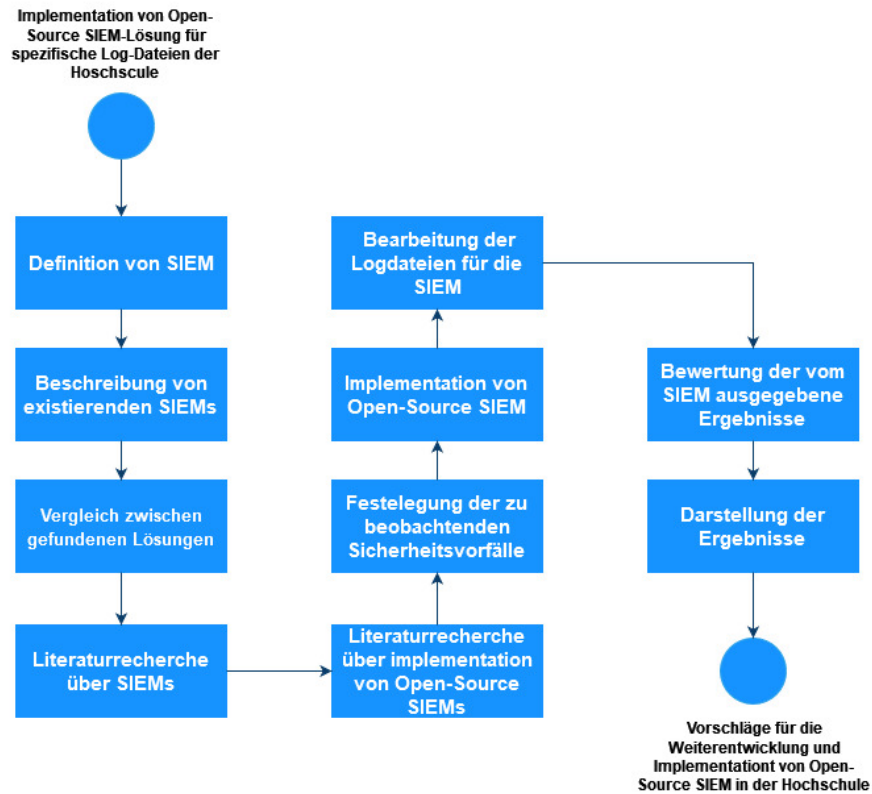


Abbildung 1: Aufbau dieser wissenschaftlichen Recherche SIEM  
Quelle: Eigene Darstellung

## 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 bearbeiten werden können.

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:

- Recherche in der Fachliteratur über SIEMs Lösungen
- Vergleich zwischen verschiedenen Open Source SIEM Tools
- Installation von virtuellen Maschinen zur Nutzung von der ausgewählten SIEM oder
- Nutzung von Container zur Installation von SIEM
- Importieren von Logdateien in der ausgewählten SIEM Lösung
- Bewertung der ausgegebenen Daten

## 2 Definition von SIEM

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, unterstützt techopedia (2022).

In dem Universum von Security Operations Center (SOC) mischen sich verschiedenen Begriffe, die manchmal zur Verwirrung führen, weil sie ähnliche Bedeutung und Verantwortung haben. Intrusion Detection System (IDS), Intrusion Prevention System (IPS) und Security Information and Event Management (SIEM) werden von *nonnative users* und sogar von Spezialisten oft verwechselt, da ihre Aufgabe mehr Zusammenhang als Unterschied haben. Um Umfang dieser Arbeit wegen der zeitlichen Einschränkungen zu verringern, fassen wir kurz die Unterschiede zwischen ihnen zusammen und legen wir unsere Grenze auf den SIEMs Lösungen fest.

Intrusion Detection System (IDS) sind Software oder Hardware die Cyberangriffe identifizieren und berichten. Sie haben eine passive Rolle, weil sie die Cyberangriffe weder stoppen noch verhindern können. Intrusion Prevention System (IPS) seinerseits haben eine aktive Haltung gegenüber Cyberangriffe, die können automatisch behandeln, indem sie Blocking-Mechanismus einschalten, um den Angriff zu stoppen (Wendzel, 2018). Wie Intrusion Detection System (IDS), kann der Intrusion Prevention System (IPS) auch Logdateien generieren, die von einer SIEM Lösung gesammelt werden kann.

Die beiden ersten können innerhalb eines Unternehmen coexistieren, müssen aber nicht. Die Datenquellen von SIEMs können, unter anderen, von diesen beiden Tools entstehen. Die folgenden Abbildung stellt didaktisch, wie sich SIEMs in diesem Landschaft integrieren lassen:

## UNDERSTANDING THE SIEM ARCHITECTURE

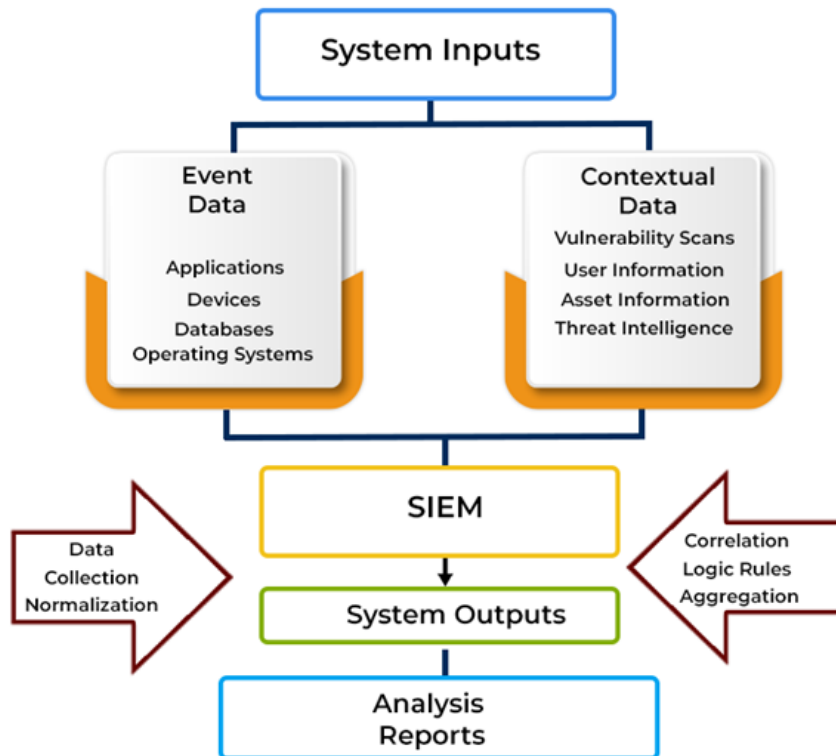


Abbildung 2: Allgemeine Informationsfluss von SIEM  
Quelle: (Mohan, 2022)

Aus dem Bild können wir feststellen, dass SIEMs für die Zentralisierung von Sicherheitsdaten zuständig ist. Diese werden dann bearbeitet und in einem oder mehreren Berichten dargestellt, damit das SOC-Team schnellere und effektive Entscheidungen treffen können. Der Informationsfluss einer SIEM Lösung können wir in der folgenden Abbildung darstellen:

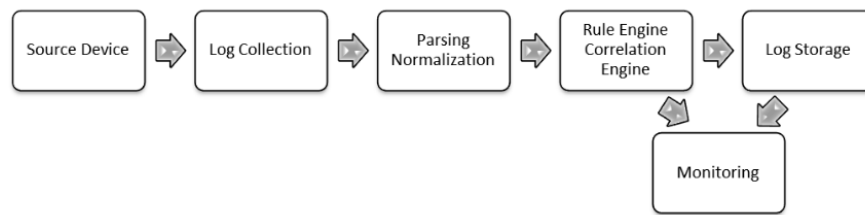


Abbildung 3: Allgemeine Informationsfluss von SIEM  
 Quelle: (Granadillo et al., 2021)

SIEM ist aber viel mehr als eine Sammlung von Logdateien. Das Ziel dieser Software ist die automatische Analyse zu ermöglichen, indem Daten kombiniert und bewertet werden können. In vielen Bereiche, wie Finanzen (Payment Card Industry Data Security Standard (PCDI DSS)), Gesundheitswesen (Health Insurance Portability and Accountability Act(HIPAA)), sind SIEMs gesetzliche Verpflichtung (Jog, 2020). In Deutschland verpflichtet das Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) Organisationen mit kritischen Infrastrukturen die Anwendungen von solche Lösungen, um Störungen der Confidentiality, Integrity and Availability (CIA) zu verhindern (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021).

## 2.1 Existierende SIEM Lösungen

Die existierenden SIEMs Lösungen können in zwei Kategorie getrennt werden: *Proprietary* und *Open Source*. Zu der ersten ist Splunk von dem Unternehmen Splunk Technology die meist verwendete Software (Kazarov et al., 2018). Da unser Fokus hier auf *Open Source* Lösungen liegt, diskutieren wir hier demnächst über folgende Software:

**Wie konnte ich Grafana hier erwähnen? Grafane ist eher allgemein und nicht so zu Alert orientiert, habe ich hier gefunden: Splunk x Grafana und hier What is Grafana**

- Prelude
- AlienVault

- ELK Stack

### 2.1.1 Prelude

aaaaaaa

### 2.1.2 AlienVault OSSIM

AlienVault OSSIM ist eine im Jahr 2007 entwickelte Open Source SIEM Lösung. Im Jahr 2018 wurde sie von der Firma AT&T Communication gekauft (CBNINSIGHTS, 2020). In der Beschreibung des Anbieters steht, dass sie auch dabei unterstützt, Daten zu sammeln, zu normalisieren und zu bewerten. Er behaupt auch, dass sein Tool in der Lage ist, Schwachstelle und Angriffe zu erkennen, Verhältnis zu beobachten und Datenzusammenhang durchzuführen (AT&T Cybersecurity, 2022).

Laut der Website Comparitech steht AlienVault in der 13ten Platz von den besten bewerteten SIEM Lösungen. Die Seite beschreibt auch, dass einen IDS, Verhaltensüberwachungssystem und einen Schwacstellescanner integriert sind . Die Anwendung ist auch mit der Plattform Open Threat Exchange(OTX) verbunden, diese ermöglicht die Teilung von Informationen über Schwachstelle. Comparitech highlighted, dass die Anwendung wegen ihre niedrigen Kosten besser für kleine oder mittelständige Unternehmen geeignet ist (comparitech, 2023).

Die Anwendung bietet konsistente Datenzusammenhang von Daten und vermeidet den Auftauch von falsch positiv. AlienVault kommt auch mit vordefinierten Use-Cases, die dabei unterstützen gewöhnlichen Angriffsszenario zu erkennen. Die Installation, die Einstellung und die Integration mit anderen Tools ist auch benutzerfreundlich (Gómez et al., 2022). Aus einer anderen wissenschaftlicher Quelle fanden wir heraus, dass es für viele Quelle eine manuelle Normalisierung der Logdateien notwendig ist Nabil et al. (2017). Die Anwendunt hat aber einen zuverlässigen Berichtsmechanismus.

positive die Anwendung

verwendeten verwendeten Wie andere SIEM Lösungen, ist AlienVault OSSIM auch mit anderen Tools integriert, um Daten zu empfangen und zu bearbeiten.

### **2.1.3 ELK Stack**

cccccccccc

### **2.1.4 Zusammenfassender Vergleich**

dddddddddd

## **2.2 Existierende SIEM Lösungen**

eeeeeeeeee

listen wir hier einige recherchierte Tools und prä

- Architektur

- Anpassung

## 3 Implementation

### 3.1 Installation von SIEM in Container

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

- Implementation in Container

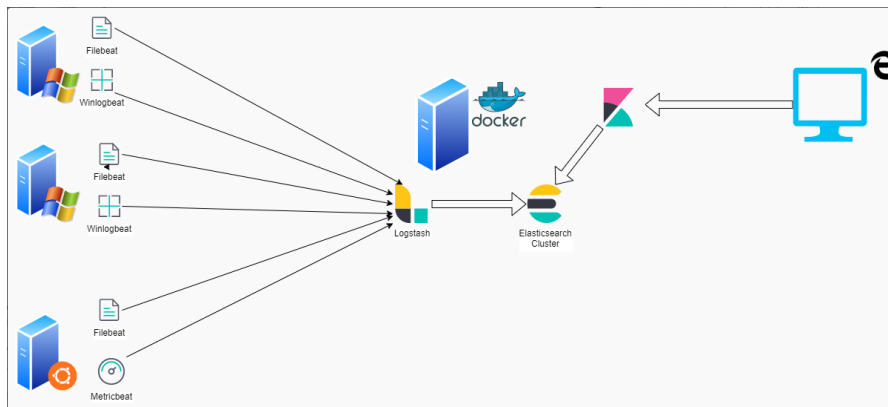


Abbildung 4: Struktur von SIEM in einem Container  
Quelle: (RDR\_IT, 2022)

### 3.2 Sammlung von Server-Log Dateien

### 3.3 Normalisierung der Log-Dateien



## **4 Fazit**

Zusammenfassung von

- Zielen
- Ergebnissen
- Herausforderungen

### **4.1 Zukünftige Entwicklungen**

## Literaturverzeichnis

- AT&T Cybersecurity (2022). Alienvault ossim.  
<https://cybersecurity.att.com/products/ossim>. Zugriff am 5.3.2023.
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2021). Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0).  
[https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it\\_sig-2-0\\_node.html](https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html). Zugriff am 4.3.2023.
- CBNINSIGHTS (2020). Alienvault.  
<https://www.cbinsights.com/company/alienvault>. Zugriff am 5.3.2023.
- Centers for Disease Control and Prevention (2016). Health Insurance Portability and Accountability Act of 1996 (HIPAA).  
<https://www.pcicomplianceguide.org/faq/>. Zugriff am 4.3.2023.
- 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.
- comparitech (2023). The best siem tools for 2023: Vendors solutions ranked.  
<https://www.comparitech.com/net-admin/siem-tools/>. Zugriff am 5.3.2023.
- 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](file:///C:/Users/bruno/Downloads/Security_Information_and_Event_Management_SIEM_Ana.pdf). Zugriff am 21.2.2023.
- Gómez, E. C. F., Almeida, O. X. B., and Gamboa, L. M. A. (2022). Analysis of centralized computer security systems through the alienvault ossim tool. *Ecuadorian Science Journal*, 6(1):23–31.
- Harmes, T. (2023). It-sicherheitsgesetz 2.0.  
<https://rz10.de/knowhow/it-sicherheitsgesetz-2-0/>. Zugriff am 4.3.2023.
- Hochschule Worms (2018). Fachspezifische prüfungsordnung (fpo 2018).  
[https://www.hs-worms.de/fileadmin/media/fachbereiche/informatik/AInf/P\\_ruefungsordnung/AnInf\\_FP0\\_2017-12-19\\_FINAL.pdf](https://www.hs-worms.de/fileadmin/media/fachbereiche/informatik/AInf/P_ruefungsordnung/AnInf_FP0_2017-12-19_FINAL.pdf). Zugriff am 11.2.2023.
- Jog, Y. (2020). Security Information and Event Management (SIEM).

- <https://www.linkedin.com/pulse/security-information-event-management-siem-yatin-jog>. Zugriff am 4.3.2023.
- Kazarov, A., Avolio, G., Chitan, A., and Mineev, M. (2018). Experience with splunk for archiving and visualisation of operational data in atlas tdaq system. *Journal of Physics: Conference Series*, 1085:032052.  
<http://dx.doi.org/10.1088/1742-6596/1085/3/032052>. Zugriff am 4.3.2023.
- 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 26.2.2023.
- Nabil, M., Soukainat, S., Lakbabi, A., and Ghizlane, O. (2017). Siem selection criteria for an efficient contextual security. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6.  
<https://doi.org/10.1109/ISNCC.2017.8072035>. Zugriff am 26.2.2023.
- Nexcess (2022). Open source vs. proprietary: Which is better?  
<https://www.nexcess.net/blog/open-source-vs-proprietary/>. Zugriff am 26.2.2023.
- NIST (2020a). Cyber attacke.  
[https://csrc.nist.gov/glossary/term/Cyber\\_Attack](https://csrc.nist.gov/glossary/term/Cyber_Attack). Zugriff am 19.2.2023.
- NIST (2020b). Cyber attacke.  
[https://csrc.nist.gov/glossary/term/security\\_information\\_and\\_event\\_management\\_tool](https://csrc.nist.gov/glossary/term/security_information_and_event_management_tool). Zugriff am 17.02.2023.
- NIST (2020c). False positive.  
[https://csrc.nist.gov/glossary/term/false\\_positive](https://csrc.nist.gov/glossary/term/false_positive). Zugriff am 05.03.2023.
- 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.
- U.S. Department of Health & Human Services (2016). The HIPAA Privacy Rule.  
<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>. Zugriff am 4.3.2023.
- Venkatramulu, S., Phridviraj, M., Srinivas, C., and Rao, V. (2021). Implementation of grafana as open source visualization and query processing platform for data scientists and researchers. *Materials Today: Proceedings*.  
<http://dx.doi.org/10.1016/j.matpr.2021.03.364>. Zugriff am 04.03.2023.
- Vielberth, M. (2021). *Encyclopedia of Cryptography, Security and Privacy*, chapter Security Operations Center (SOC), pages 1–3. Springer Berlin Heidelberg.  
[http://dx.doi.org/10.1007/978-3-642-27739-9\\_1680-1](http://dx.doi.org/10.1007/978-3-642-27739-9_1680-1). Zugriff am 04.03.2023.
- 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.