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

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

Graphical user interface (GUI) eine Schnitstelle, die den Nutzer ermöglicht, mithilfe von Symbolen und visuellen Elementen mit der Anwendung zu interagieren (Fu, 2018).

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

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

Network Operations Center (NOC) zentraliserter Bereich eines Unternehmens dafür zuständig, Netzwerkaktivitäten zu überwachen und zu verwalten (Mohammed et al., 2021) .

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

Security Operations Center (SOC) zentraliserter Bereich eines Unternehmens dafür zuständig, Sicherheitsvorfälle zu überwachen, zu identifizeren, 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, modifiziren und verbreiten können, ohne dafür Lizenzen bezahlen zu müssen (Open Source Initiative, 2007).

Plugin optionale Software-Komponenten, die weitere Funktionalitäten zu einer Anwendung hinzufügen (IT-Service.Network, 2020).

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).

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme ein im Jahr 2021 verabschiedetes Bundesgesetz zur Erhöhung von Sicherheit informationstechnischen Systemen besonders, solchen von den kritischen Infrastrukturen (Harmes, 2023).

Abkürzungsverzeichnis

CIA Confidentiality, Integrity and Availability.

FPO Fachspezifische Prüfungsordnung.

GUI Graphical user interface.

HIPAA Health Insurance Portability and Accountability Act.

IDS Intrusion Detection System .

IPS Intrusion Prevention System .

KI Künstliche Intelligenz.

LML Log Monitoring Lackey.

NIST National Institute of Standards and Technology.

NOC Network Operations Center.

OSSIM Open Source Security Information Management .

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.

USM Unified Security 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. 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:

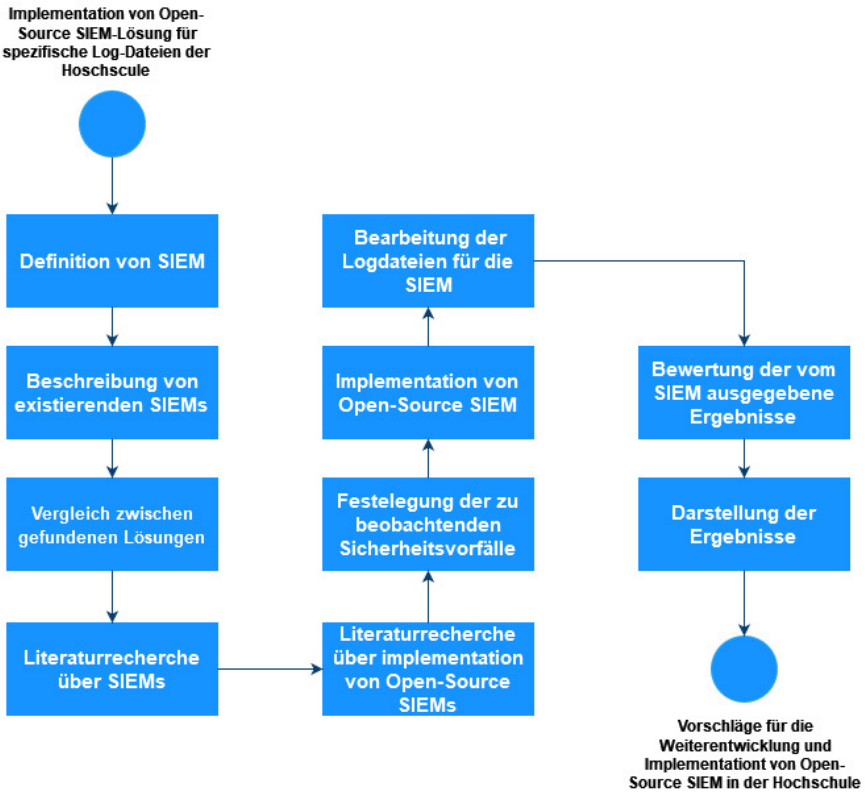

Abbildung 1: Aufbau dieser wissenschaftlichen Recherche SIEM
Quelle: Eigene Darstellung

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, untersützt 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 verringen, 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 identifzieren 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:

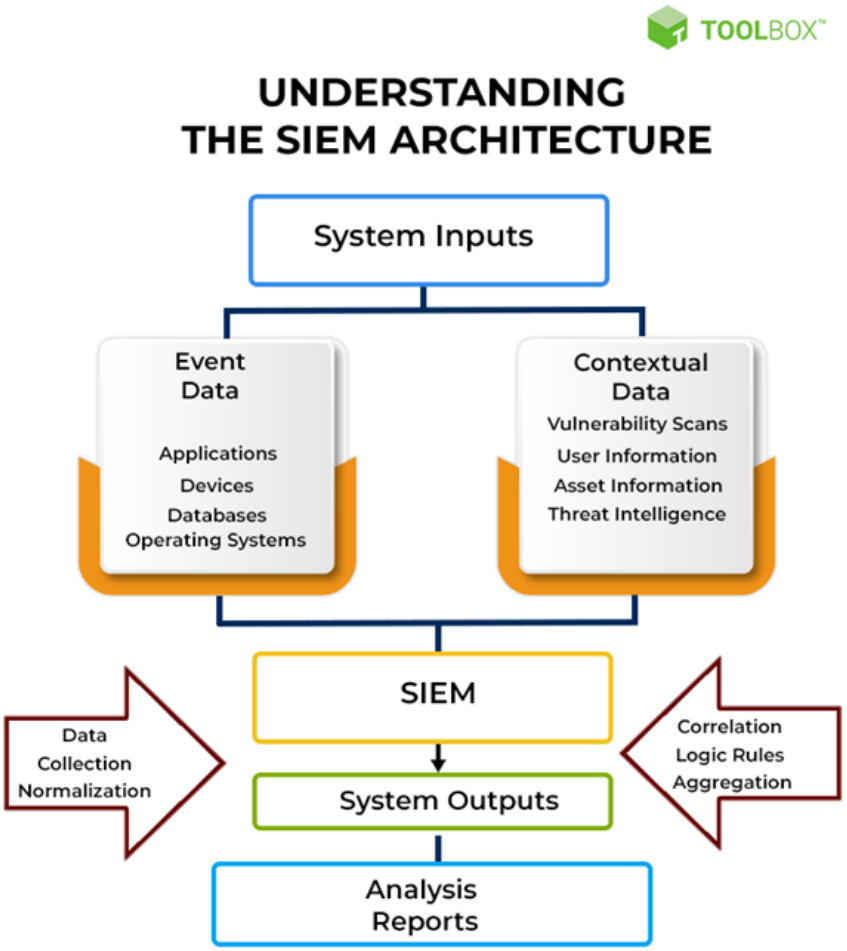

Abbildung 2: Allgemeine Informationsfluss von SIEM
Quelle: (Mohanan, 2022)

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 wirder in der folgenden Abbildung darstellen:

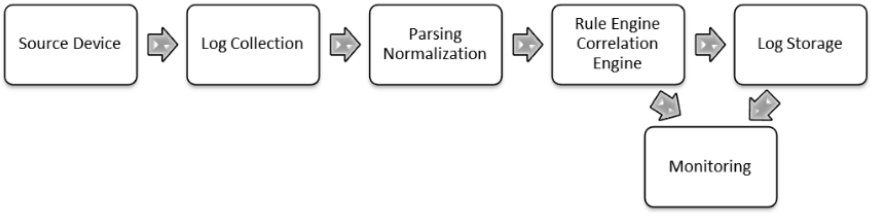

Abbildung 3: Allgemeine Informationsfluss von SIEM
Quelle: (Granadillo et al., 2021)

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 verplichtet das Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme 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 algemmein und nicht so zu Alert orientiert, habe ich hier gefunden: Splunk x Grafana und hier What is Grafana

- Prelude
- AlienVault Open Source Security Information Management (OSSIM)

- FortiSIEM
- ELK Stack

2.1.1 Prelude

Das im Jahr 2002 in Frankreich von Yoann Vandoorselaere freigegebene Tool Prelude zählt zu gehört zu einer europäischen Open Source SIEM Lösung. Laut dem Anbieter verfügt Prelude unter anderen folgenden Funktionalitäten (Prelude SIEM, 2018):

- Informationszentralisierung
- Datenaggregation und -Zusammenhang mit vordefinierten und von den Nutzer angepassten Regeln
- Einbruchserkennungmechanismen
- Datennormalisierung

Die Anwendung besteht aus verschiedenen unabhängige Modulen. Unter denen highlighten wir folgende: Warnmeldung, Archivierung, Analyse und Verwaltung. Das erste gehört zu der zentrallen Aufgabe dieser Lösung, es ist dafür zuständig, Daten zu empfangen, zu normalisieren, Zusammenhang zu machen und Meldungen zu generieren. Das zweite Modul, Archivierung, konzentriert sich auf die Speicherung und Verfügbarkeit der Daten. Zu der Analyse-Modul gehören statistische Aufgabe und Darstellung in verschiedenen Formaten. Das letzte Modul dient dazu, die Anwendung zu steuern, Nutzer zu erstellen dessen Rechts zu konfigurieren (European Comission, 2015).

Die folgende Abbildung zeigt die Integration der verschiedenen Module von Prelude und wie sie sich kommunizieren, um Analyse, Meldung und Speicherung zu generieren:

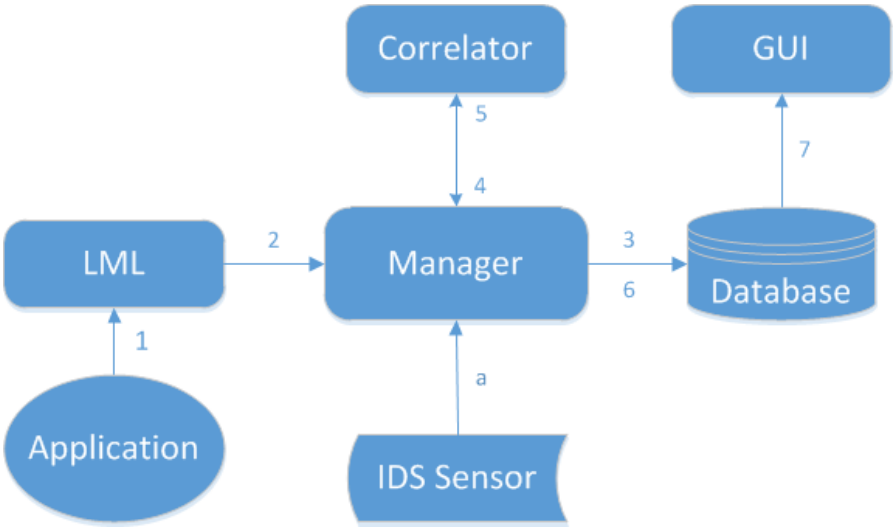

Abbildung 4: Integration zwischen den Modulen von Prelude
Quelle: (Prelude Team, 2007)

Aus der Abbildung und der Dokumentation können wir folgende Informationsfluss: die Daten werden von Endanwendung genieriert und zum Loganalyzer (Prelude Log Monitoring Lackey (LML)) geschickt, wo sie normalisiert und bewertet sind. Für solche Logs, wo es verdächtige Werte gibt, werden Warnmeldung genieriert. Diese Meldung wird zum Manager Module weitergeleitet. Der Correlator oben sucht nach Zusammenhang zwischen andere Daten. Das Ergebnis von Correlator ist wieder zum Manager geschicht und danach zu dem Datenbank. Schließlich stehen die Berichte in dem User-Interface zur Verfügung (Prelude SIEM, 2020).

Die Architektur der Anwendung ermöglicht sowohl einen zentraliserter als auch einen desentralisierten Aufbau. In der nächsten Abbildung sehen wir eine einfache Implementation von Prelude:

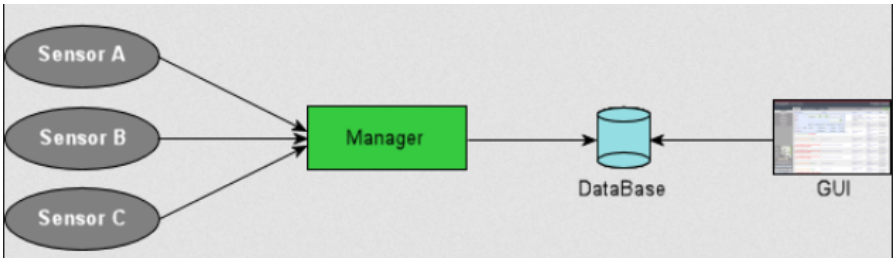

Abbildung 5: Einfache Architektur von Prelude
Quelle: (Prelude Team, 2007)

In einer desentralisierte Umgebung werden Daten von verschiedenen und getrennte Quellen generiert und bearbeitet. Schließlich können die Nutzer auf diesen Daten unter einem GUI zugreifen.

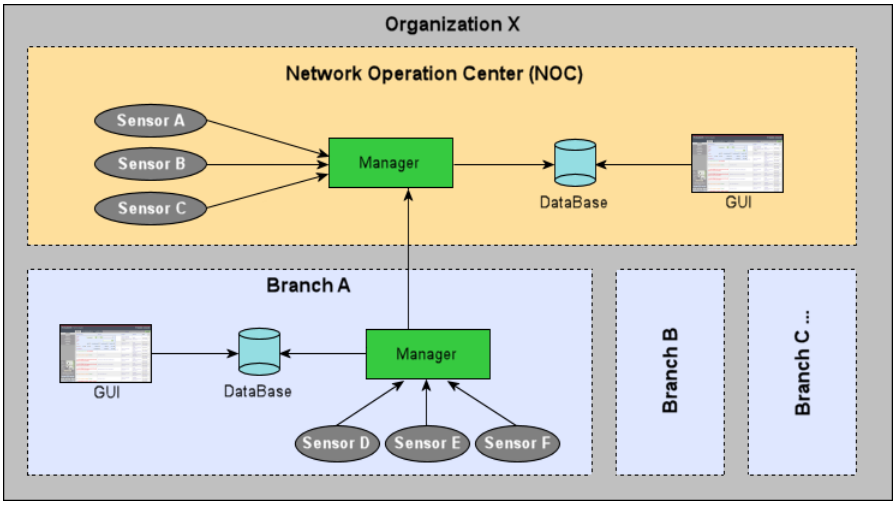

Abbildung 6: Erweiterte Architektur von Prelude mit der Nutzung von dezentralisierten Datenquellen und Bearbeitung
Quelle: (Prelude Team, 2007)

Die wissenschaftliche Literatur über Prelude ist sehr eingeschränkt. Wenige Publikationen fokussieren sich auf die Entwicklung, Implementation und unternehmerische Anwendung dieses Tools. Eine Studie von 2021 versuchte dieses und zwei andere Tools (AlienVault und Cyberoam iView) anhand technischer und nutzerfreundliche Kriterien zu vergleichen. Unter diese Kriterien highlighten wir folgende (Radoglou-Grammatikis et al., 2021):

- **technische Kriterien**
  - *Real-time performance*,
  - *Range and flexibility of reporting*
  - *Alert correlation*
- **nutzerfreundliche Kriterien**
  - *Documentation comprehensiveness*
  - *Complexity of the installation process*
  - *Complexity of the system configuration*

In den technische Kriterien lag Prelude an dritten Platz und in den nutzerfreundliche Kriterien bekam Prelude den ersten Platz.

Auch in den nicht wissenschaftlichen Publikationen existieren begrenzte Anzahl von Texten über Preludes. Die existierenden kommentieren ganz zusammenfassend über die ausreichende Dokumentation und heben hervor, dass es eher eine in Europa konzentrierte Lösung.

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 untersützt, 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).

AlienVault hat eine kostenpflichtige Version, die Alien Vault Unified Security Management (USM) heißt. In der Webseite von AT&T steht, dass es keine spezifische Dokumentation für die Open Source Version, AlienVault OSSIM, gibt, weil viele Funktionalitäten von der anderer Version stammen (AT&T Cybersecurity, 2022).

Die folgende Abbildung zeigt das von dem Anbieter freigelegte Architektursdiagramm von der USM Version:

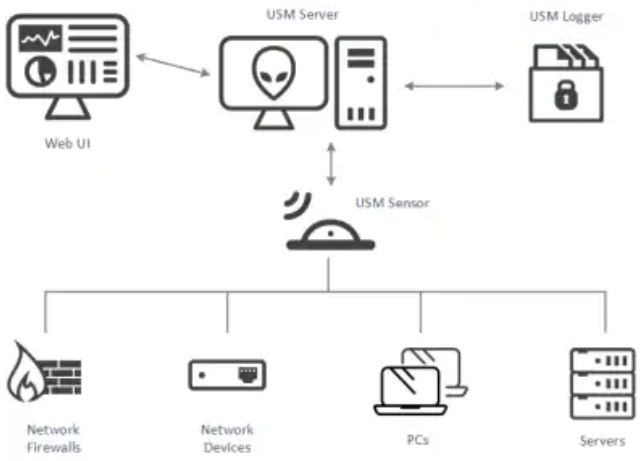

Abbildung 7: Architekturdiagram von AlienVault USM
Quelle: (AT&T Cybersecurity, 2022)

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 Platform Open Threat Exchange(OTX) verbunden, diese ermöglicht die Teilung von Informationen über Schwachstelle. Comparitech highlighted, dass die Anwendung wegeren ihre nidriegen Kosten besser für kleine oder mittelständige Unternehmen geignet ist (comparitech, 2023).

Die Anwendung soll konsitenten Datenzusammenhang anbienten und soll den Auftauch von falsch positiv vermeiden. 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 Logdatein notwendig ist Nabil et al. (2017). Die Anwendunt hat aber einen zuverlässigen Berichtsmechanismus.

Während unserer Recherche gab es wenige wissenschaftliche Literatur, die sich um AlienVault OSSIM kümmert. Kommerzielle Publikationen waren auch viel auf die Firma AT&T auf die kostenpflichtige Version des Tools konzentriert.

2.1.3 FortiSIEM

FortiSIEM ist eine US-amerikanische SIEM Lösung von der Firma Fortinet. Fortinet kaufte im Jahr 2016 das Unternehmen AccelOps und dessen SIEM Lösung und unbenant es zum FortSIEM (Fortinet, 2016).

Laut dem Anbieter hat FortiSIEM eine robuste Integration mit anderen Tools und lässt sich leicht und einwandfrei skalieren. Andere Versionen des Tools sind mit Machine Learning integriert, sodass die Anwendung auch verhältnisanalyse durchführen kann (Fortinet, 2022). Das Tool bietet auch eine extensive und ausführliche Dokumentation an. Die nächste Abbildung zeigt die skalierbare Architektur des Tools:

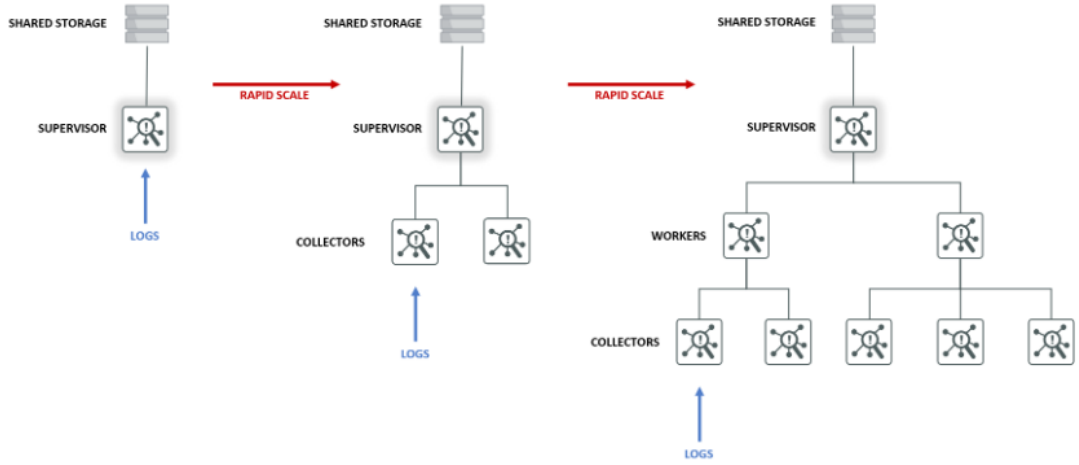

Abbildung 8: Skalierbare Architektur von FortiSIEM
Quelle: (Fortinet, 2020)

Auch zu dieser SIEM Lösung ist die wissenschaftliche Produktion eingeschränkt. Eine von der gefundenen Publikation betonnt, dass FortiSIEM eine schnelle Erkennung von Angriff anbietet und über Network Operations Center (NOC) Funktionalitäten verfügt

(Ramírez Tomás, 2018). Wie andere SIEMs Lösungen hat FortiSIEM folgende Funktionalitäten:

- Datensammlung und Normalisierung
- Datenzusammenhang
- Generierung von Berichten
- Warnmeldungen
- Datenbewertung

2.1.4 ELK Stack

ELK Stack stammt aus der Verbindung von drei Open Source Tools: Elasticsearch, Logstash, and Kibana. Das erste ist eine Such- und Analysemaschine. Das zweite ist eine Server-Seite Anwendung zur Datenverarbeitung und -Weiterleitung. Schließlich Kibana ist dafür zuständig, visuelle Darstellung in Graphikformat auszugeben (packt, 2019). Dieses Tool besitzt viele Eingeschaften von einer SIEM-Lösung und ist von vielen SOC verwendet, ist aber, für viele Experten, kein SIEM für sich, da es über keine Warnmeldungsystem, Datenzusammenhang und Vorfälleverwaltung verfügt (Miller, 2021). Diese und anderen Funktionalitäten lassen sich aber durch Plugins integrieren.

Das folgende Diagram stellt die Architektur von ELK Stack mit ihren integrierten Elementen dar:

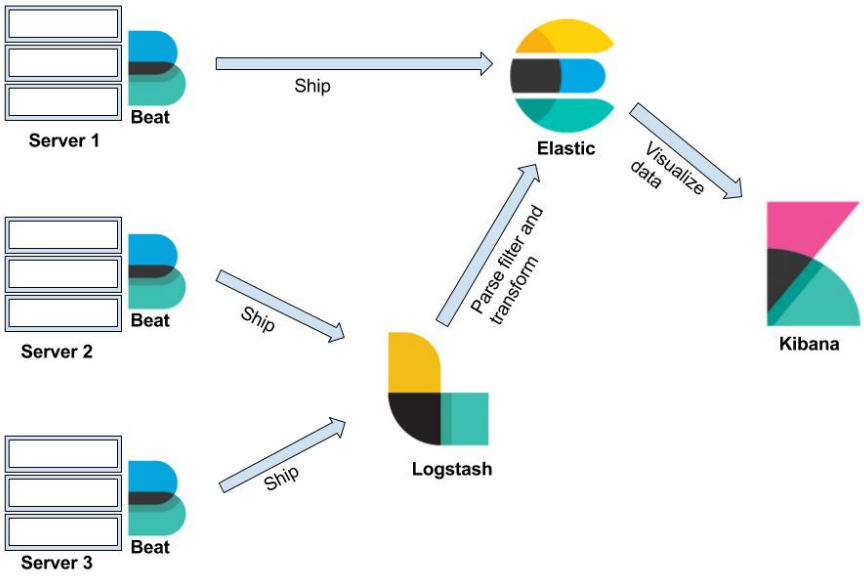

Abbildung 9: Integration zwischen Elasticsearch, Logstash und Kibana
Quelle: (packt, 2019)

Auf dem Bild werden auch Beats gezeigt. Diese Komponenten sind an der Endanwendung installiert und sie leiten Daten entweder zu Elasticsearch oder zu Logstash weiter, wo sie Schließlich bearbeitet werden (Jain, 2018).

Ein Teil der wissenschaftlichen Literatur highlight die Logsanalyse-Funktionalitäten von ELK Stack und die Unterstützung bei Normalisierung und Indexierung von Daten für eine lesbare Ausgabe (Advani et al., 2020). Die starke Skalierbarkeit wurde auch bei einer Studie erwähnt, wo ELK Stack für Wi-Fi Logging eingesetzt wurde wurde (Wang et al., 2019).

Die offiziele Dokumentation von ELK Stack betonnt, dass die Anwendung folgende Funktionalitäten besitzen: mit der Anwendung folgendes möglich ist (elastic, 2022):

- Datensuche, -Normalisierung, -Analyse und
- Speicherung
- visuelle Ausgabe

Folgendes Diagram aus der offizielen Dokumentation zeigt die Aufteilung der Funktionalitäten por Element von ELK Stack:

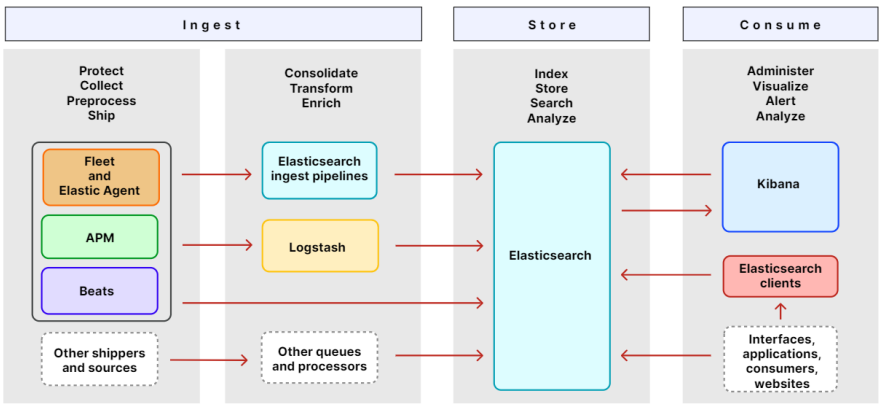

Abbildung 10: Aufteilung der Funktionalitäten zwischen den Komponenten
Quelle: (elastic, 2022)

Die wissenschaftliche Publikation über ELK Stack ist vielfältiger als bei der anderen recherchierten Tools. Es ist aber wichtig, zu betonen, dass die Mehrheit von denen sich eher mit den Logging als mit den SIEM-Eingeschaften der Anwendung beschäftigen.

2.2 Auswahlkrietieren

Die wichtigste Kriteria für unsere Auswahl war, dass die Anwendung Open Source sein sollte. Kostenpflichtige Versionen können wegen ihrem Preis und Komplexität besonders kleinere Unternehmen abschrecken und infolgendessen bleiben sie fern von einigen Sicherheitslösungen (Bjørk, 2022).

Für diese haben entschieden wir uns für die XXXXX SIEM Lösung aus folgenden Gründen:

- eingeschränkte Ressource für die Entwicklung dieser Arbeit
- bbbbbbbbbbbbbb
- ccccccccccccc

- ddddddddddddddd
- eeeeeeeeeeeeeee

Demnächst fokussieren wir uns in der Installation, Konfiguration und Implementation von XXXXXX. Danach werden wir spezifische Logdateiein der Hochschule importieren, normalisieren und diese anhand Angriff1 und Angriff2 beobachten.

3 Implementation

3.1 Installation von SIEM in Container

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

- Implementation in Container

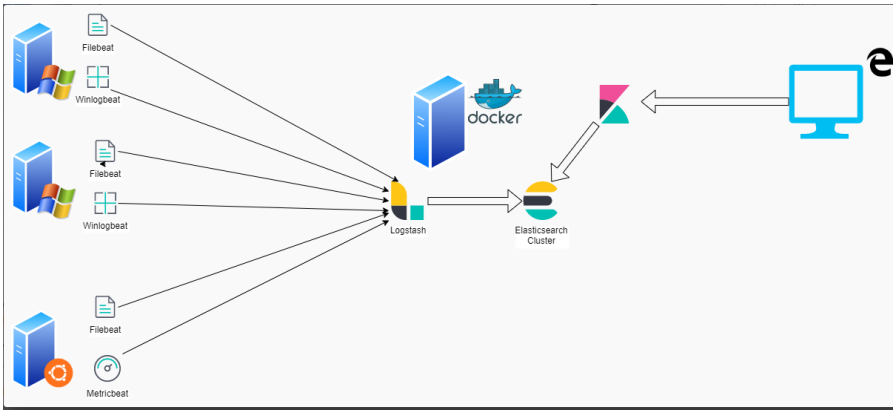

Abbildung 11: Struktur von SIEM in einem Container
Quelle: (RDR_IT, 2022)

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

Advani, S., Mridul, M., Vij, P. S. R., Agarwal, M., and A., L. P. (2020). Iot data analytics pipeline using elastic stack and kafka. *International Journal of Computer Sciences and Engineering*, 8:144–148.
https://www.ijarcce.com/upload/2016/april-16/IJARCCE%2013.pdf. Zugriff am 7.3.2023.

AT&T Cybersecurity (2022). Alienvault ossim.
https://cybersecurity.att.com/products/ossim. Zugriff am 5.3.2023.

Bjørk, R. (2022). *Feasibility to implement a SIEM based on Open-source applications*. PhD thesis, KTH Royal Institute of Technology.
https://kth.diva-portal.org/smash/get/diva2:1668180/FULLTEXT01.pdfl. Unpublished thesis. Zugriff am 6.3.2023.

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. 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.

elastic (2022). *Elastic Docs*.
https://www.elastic.co/guide/en/welcome-to-elastic/current/new.html. Zugriff am 15.8.2023.

European Comission (2015). Siem design and development.
https://cordis.europa.eu/project/id/644425. Zugriff am 5.3.2023.

Fortinet (2016). Fortinet Announces Acquisition of AccelOps .
https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2016/fortinet-announces-acquisition-of-accelops. Zugriff am 6.3.2023.

Fortinet (2020). FortiSIEM Reference Architecture.
https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/DeploymentGuide/dg-fortisiem-reference-architecture.pdf. Zugriff am 6.3.2023.

Fortinet (2022). FortiSIEM Solutions.
https://www.fortinet.com/products/siem/fortisiem. Zugriff am 6.3.2023.

Fu, F. (2018). Chapter six - design and analysis of complex structures. In *Design and Analysis of Tall and Complex Structures*, pages 177–211. Butterworth-Heinemann.
https://www.sciencedirect.com/science/article/pii/B978008101018100006X. Zugriff am 6.3.2023.

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.

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.
https://journals.gdeon.org/index.php/esj/article/view/181. Zugriff am3.3.2023.

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/Pruefungsordnung/AnInf_FPO_2017-12-19_FINAL.pdf. Zugriff am 11.2.2023.

IT-Service.Network (2020). Was ist ein plug-in?
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. Zugriff am 4.3.2023.

Jain, U. (2018). *Lateral Movement Detection Using ELK Stack*. PhD thesis, University of Houston.
https://uh-ir.tdl.org/handle/10657/3109. Zugriff am 7.3.2023.

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.

Miller, J. (2021). is elastic stack (elk) the best siem option? https://www.bitlyft.com/resources/is-elk-the-best-siem-option#:~:text=The%20ELK%20stack%20is%20a,system%20from%20a%20system%20provider. Zugriff am 7.3.2023.

Mohammed, S. A., Mohammed, A. R., Côté, D., and Shirmohammadi, S. (2021). A machine-learning-based action recommender for network operation centers. *IEEE Transactions on Network and Service Management*, 18(3):2702–2713. https://doi.org/10.1109/TNSM.2021.3095463. 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. Zugriff am 19.2.2023.

NIST (2020b). Cyber attacke. 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. Zugriff am 05.03.2023.

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

packt (2019). What is elk stack? https://subscription.packtpub.com/book/big-data-and-business-intelligence/9781788831031/1/ch01lvl1sec10/what-is-elk-stack. Zugriff am 7.3.2023.

Prelude SIEM (2018). [prelude siem: Smart security]. https://www.prelude-siem.com/en/prelude-siem-en/. Zugriff am 5.3.2023.

Prelude SIEM (2020). *Prelude Documentation: version 5.2*.

https://www.prelude-siem.org/docs/5.2/en/. Zugriff am 6.3.2023.

Prelude Team (2007). *Manual User*.
https://www.prelude-siem.org/projects/prelude/wiki/. Zugriff am 6.3.2023.

Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulias, A., Angelopoulos, M., and Ramos, F. (2021). Spear siem: A security information and event management system for the smart grid. *Computer Networks*, 193:108008.
https://doi.org/10.1016/j.comnet.2021.108008. Zugriff am3.3.2023.

Ramírez Tomás, I. (2018). *Implementación de un sistema de gestión de eventos de seguridad en una empresa de tamaño medio*. PhD thesis, Universitat Politècnica de València.
https://riunet.upv.es/bitstream/handle/10251/109765/Ram%c3%adrez%20-%20Implementaci%c3%b3n%20de%20un%20sistema%20de%20gesti%c3%b3n%20de%20eventos%20de%20seguridad%20en%20una%20empresa%20de%20tama%c3%b1....pdf?sequence=1&isAllowed=y. Zugriff am 06.03.2023.

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. Zugriff am 04.03.2023.

Wang, Y.-T., Yang, C.-T., Kristiani, E., and Chan, Y.-W. (2019). The implementation of wi-fi log analysis system with elk stack. In *Frontier Computing*, pages 246–255, Singapore. Springer Singapore.
`https://link.springer.com/chapter/10.1007/978-981-13-3648-5_28`. Zugriff am 07.03.2023.

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.