

**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>4</b>
<b>Abbildungsverzeichnis</b>	<b>5</b>
<b>Glossar</b>	<b>6</b>
<b>Abkürzungsverzeichnis</b>	<b>10</b>
<b>1 Einleitung</b>	<b>12</b>
1.1 Problemstellung . . . . .	14
1.2 Vorgehensweise . . . . .	15
<b>2 Definition von SIEMs und Log Analysis Tools</b>	<b>16</b>
2.1 Existierende SIEMs Lösungen und Log Analysis Tools . . . . .	19
2.1.1 Splunk . . . . .	20
2.1.2 Prelude . . . . .	21
2.1.3 AlienVault OSSIM . . . . .	24
2.1.4 FortiSIEM . . . . .	26
2.1.5 ELK-Stack . . . . .	27
2.1.6 Grafana . . . . .	29
2.2 Auswahlkriterien . . . . .	31
<b>3 Implementation</b>	<b>32</b>
3.1 Angriffserkennung mithilfe von Mitre ATT&CK Matrix® . . . . .	33
3.2 Aufbau der Erkennungsregel für den ausgewählten Angriff . . . . .	36
3.3 Bewertung der Daten in Grafana . . . . .	37
3.4 Normalisierung der Logdateien mit Zeek . . . . .	37
3.5 Sammlung von Server-Log Dateien . . . . .	37
3.6 Normalisierung der Log-Dateien . . . . .	37

<b>4</b>	<b>Fazit</b>	<b>38</b>
4.1	Zukünftige Entwicklungen . . . . .	38
	<b>Literaturverzeichnis</b>	<b>39</b>

## Abstract

XXXXXXXXXXXXXXXXXXXX

## Abbildungsverzeichnis

1	Aufbau dieser wissenschaftlichen Recherche Security Information and Event Management (SIEM) Quelle: Eigene Darstellung . . . . .	14
2	Allgemeine Struktur von SIEM Quelle: (Mohanam, 2022) . . . . .	17
3	Allgemeine Informationsfluss von SIEM Quelle: (Granadillo et al., 2021) .	18
4	Allgemeine Struktur von Log Analysis Tools Quelle: (Tek-Tools, 2020) . .	18
5	Allgemeine Informationsfluss von Log Analysis Tools Quelle: (neptune, 2023) . . . . .	18
6	Integration zwischen den Modulen von Prelude Quelle: (Prelude Team, 2007) . . . . .	21
7	Einfache Architektur von Prelude Quelle: (Prelude Team, 2007) . . . . .	22
8	Erweiterte Architektur von Prelude mit der Nutzung von dezentralisierten Datenquellen und Bearbeitung Quelle: (Prelude Team, 2007) . . . . .	23
9	Architekturdiagramm von AlienVault Unified Security Management (USM) Quelle: (AT&T Cybersecurity, 2022) . . . . .	25
10	Skalierbare Architektur von FortiSIEM Quelle: (Fortinet, 2020) . . . . .	26
11	Integration zwischen Elasticsearch, Logstash und Kibana Quelle: (packt, 2019) . . . . .	28
12	Aufteilung der Funktionalitäten zwischen den Komponenten Quelle: (elastic, 2022) . . . . .	29
13	Integration von verschiedenen Log-Quellen mit Grafana Loki Quelle: (Grafana Labs, 2022) . . . . .	30
14	Aufbau unseres Arbeitslabors Quelle: Eigene Quelle . . . . .	32
15	Erwarteter Ablauf von der Datensammlung bis zur Warnmeldung von Cyberangriffe Quelle: Eigene Quelle . . . . .	33
16	Struktur der Mitre Matrix Cyberangriffe Quelle: Eigene Quelle . . . . .	34
17	Analysestruktur für diese Arbeit Cyberangriffe Quelle: Eigene Quelle und (MITRE ATT&CK, 2020) . . . . .	36

18	Allgemeiner Ablauf eines Anmeldeverfahrens Quelle: Eigene Quelle und (Selvaganesh et al., 2022) . . . . .	36
----	--	----

## Glossar

**Brute-Force Angriffe** systematischer Versuch, Credentials oder andere sensitive Daten zu raten, indem verschiedene Buchstaben, Ziffern und Symbolen kombiniert werden (Sowmya et al., 2012). 15, 30, 31

**Container** funktionieren ähnlich wie vm, mit dem Unterschied, dass Container ab dem Software-Ebene entstehen. Containers werden meistens für einzelne Anwendungen verwendet, sie benutzen die Resource der Host-Maschine, haben aber eine isolierte Umgebung mit den notwendigen Resource für den Lauf der ausgewählten Anwendung (Douglass and Nieh, 2019). 27

**Cyberangriff** - Angriffe, die über Cyberspace stattfinden. Solche Angriffe zielen auf Unternehmen und deren Infrastrukturen, um sie zu zerstören, zu lähmen, zu kontrollieren oder die Integrität ihrer Daten zu stehlen oder zu dominieren (NIST, 2020b). 7, 12, 27–29, 31

**Confidentiality, Integrity and Availability (CIA)** beschreiben die drei wichtigsten Schutzziele der IT-Sicherheit: Vertraulichkeit, Integrität und Verfügbarkeit (Wendzel, 2018). 14

**Cyber Kill Chain®(CKC®)** auch *Cyberattack Lifecycle* genannt, bezieht sich auf ein Sicherheitsmodell für die Identifizierung, Analysis und Unterbrechung von fortgeschrittenen Cyberangriffen. Dieses Modell hat sieben festgelegte Phasen: *Reconnaissance*, *Weaponization*, *Delivery*, *Exploitation*, *Installation*, *Command & Control (C2)* und *Actions on Objectives* (Martin, 2018). 15, 28

**Cybersicherheit** - Diese Domäne umfasst Kenntnisse und Methoden für den Schutz, Prävention, Wiederherstellung von elektronischen Kommunikationsmitteln und deren Inhalt. Es konzentriert sich auf ihrer Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit und Verbindlichkeit (NIST, 2020b). 29

**Endpoint** bezieht sich auf Geräte oder Systeme, die mit dem Netzwerk verbunden sind. Diese können z.B. Handys, Servers, Computers, Sensoren sein (Microsoft Security, 2022). 11, 12, 23

**Hashwerte** sind Zeichen, die aus der Ergebnis einer mathematischen Funktion (Hashfunktion) auf einem Text oder auf einer Datei entstehen. Die Wiederherstellung des originalen Objekts soll aber schwierig sein (Wendzel, 2018). 30

**Falsch Positiv** ist eine aus einer fehlerhaften erkannten Verwundbarkeit Warnmeldung (NIST, 2020b). 20

**Graphical User Interface (GUI)** ) ist eine Schnittstelle, die den Nutzer ermöglicht, mithilfe von Symbolen und visuellen Elementen mit der Anwendung zu interagieren (Fu, 2018). 17

**Health Insurance Portability and Accountability Act (HIPAA)** ist ein US-Bundesgesetz über den Schutz von sensiblen personenbezogenen Gesundheitsdaten (U.S. Department of Health & Human Services, 2016). 14

**Multi-Faktor-Authentisierung (MFA)** bezeichnet das Authentifizierungsverfahren, indem zwei oder mehrere unabhängige Komponenten zur Authentifizierung verwendet werden, z.B. ein Passwort zusammen mit dem Fingerabdruck, oder eine Karte zusammen mit der Erkennung des Muster der Iris im Auge (Ibrokhimov et al., 2019). 31

**Machine Learning (ML)** bezieht sich auf die Fähigkeit von Systemen, automatisch Probleme zu lösen und spezifische Aufgabe zu erledigen mithilfe von Datenbeziehung und Bearbeitung (Janiesch et al., 2021). 15, 21

**Mitre ATT&CK®** Abkürzung für *Adversarial Tactics, Techniques and Common Knowledge*. Es bezieht sich auf eine weltweit zugängliche Wissensbasis mit detaillierter Beschreibung, Klassifizierung und Bekämpfung von verschiedenen Angriffstechni-



ken (MITRE ATT&CK, 2018a). 7–9, 26–29

**National Institute of Standards and Technology (NIST)** ist eine US-Behörde, die für die Regelungen, Vereinheitlichung und Weiterentwicklung im Bereich Informationstechnologie zuständig ist (NIST, 2020a). 7

**Open Source** beschreibt einen Code, an den jeder zugreifen, modifizieren und verbreiten kann, ohne dafür Lizenzen bezahlen zu müssen (Open Source Initiative, 2007). 7, 11, 14, 16, 19, 22, 26

**Password Spraying** ist ein Angriff gegen Anmeldedaten, indem mögliche Passwörter gegen verschiedenen viele Benutzernamen verwendet werden. Das Ziel dieses Angriffs ist eine Kontosperrung zu vermeiden. (Swathi, 2022). 30

**Password Stuffing** ist ein Angriff gegen Passwörter, indem schon bekannte Anmeldedaten von vorherigen Angriffen verwendet werden. Dieser Angriff basiert sich auf die Idee, dass Nutzer dasselbe Passwort für verschiedenen Systemen verwenden (Ba et al., 2021). 30

**Payment Card Industry Data Security Standard (PCDI DSS)** sind Sicherheitsstandards, die Unternehmen, die Kreditkarte akzeptieren, bearbeiten, speichern oder übertragen, anwenden müssen (Centers for Disease Control and Prevention, 2016). 14

**Network Operations Center (NOC)** ist ein zentralisierter Bereich eines Unternehmens und dafür zuständig, Netzwerkaktivitäten zu überwachen und zu verwalten (Mohammed et al., 2021). 22

**Plugin** sind optionale Software-Komponenten, die weitere Funktionalitäten zu einer Anwendung hinzufügen (IT-Service.Network, 2020). 22, 24

**Proprietary** bezieht sich auf Software, die einer Firma oder Person gehören. Für die Nutzung ist meistens Kauf einer Lizenz notwendig. In diesem Fall haben Kunden wenig oder kaum Zugang zu einem originellen Code (Nexcess, 2022). 7, 14, 26

**Security Operations Center (SOC)** ist ein zentralisierter Bereich eines Unternehmens und dafür zuständig, Sicherheitsvorfälle zu überwachen, zu identifizieren, zu bewerten und dazu zu reagieren (Vielberth, 2021). 7, 11

**Use Cases** beschreiben die Interaktion zwischen Systemen und Benutzer. Sie dienen zu der Anforderungserhebung eines Systems (Savic et al., 2012). 9, 15, 26

**virtuelle Maschine (VM)** ist eine Kopie der Hardware-Struktur mit eigenen Aufteilung von Resources und mit eigenen Betriebssystem. In einer physikalischen Maschine, auch Host virtuelle Maschine genannt, kann mehreren von solchen VMs laufen. Sie emulieren ein echtes und unabhängiges System (Tanenbaum, 2009). 27

## Abkürzungsverzeichnis

**BSI** Bundesamt für Sicherheit in der Informationstechnik.

**CIA** Confidentiality, Integrity and Availability.

**CKC®** Cyber Kill Chain.

**IDS** Intrusion Detection System.

**GUI** Graphical user interface.

**IPS** Intrusion Prevention System.

**FPO** Fachspezifische Prüfungsordnung.

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

**KI** Künstliche Intelligenz.

**MFA** Multi-Faktor-Authentisierung.

**ML** Machine Learning.

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

**OTX** Open Threat Exchange.

**LML** Log Monitoring Lackey.

**OSSIM** Open Source Security Information Management.

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

**NOC** Network Operations Center.

**owasp®** Open Web Application Security Project®.

**SIEM** Security Information and Event Management.

**SEM** Security Event Management.

**SIM** Security Information Management.

**SOC** Security Operations Center.

**USM** Unified Security Management.

**VM** virtuelle Maschine.

# 1 Einleitung

Der heutige Netzwerkverkehr fast tausendfach größer als vor 20 Jahre (Roser et al., 2015). Das Internet wird heutzutage für fast alle unseren alltäglichen Tätigkeiten verwendet: Soziale Netzwerke, Video und Audio-Streaming, Einkauf, behördliche Angelegenheiten und viele andere. So viel Verkehr generiert eine unermessliche Menge von Daten, die alle möglichen Inhalte beinhalten, von unschuldigen Anfragen nach einem eigenen Kontostand bis zur Ausführung von beabsichtigten Anfragen, um Systeme lahmzumachen. Um das Erste vom Zweiten zu unterscheiden, verwenden viele Firmen das sogenannte Security Information and Event Management (SIEM) oder die Log Analysis Tools.

Das National Institute of Standards and Technology (NIST) definiert SIEM als Software für die Sammlung, Anpassung, Analyse, Überwachung und Bedrohungserkennung von Sicherheitsdaten aus verschiedenen Quellen, damit das zuständige Security Operations Center (SOC) Maßnahmen ergreifen kann (NIST, 2020b). Die Bewertung dieser Daten spielt eine wesentliche Rolle bei solchen Anwendungen, da es entscheidend ist zu wissen, ob es sich um normale Anfrage oder um Cyberangriffe handelt. Log Analysis und Log Management beziehen sich auf die Sammlung, Bearbeitung, Speicherung und/oder Löschen, Weiterleitung und Überwachung von Loginformationen. In dieser Arbeit benutzen wir den Begriff “Log Analysis Tool”, um diese Systeme zu referenzieren.

In diesem Projekt recherchieren und vergleichen wir existierende SIEM und Log Analysis Tools. Danach entscheiden wir uns für eine Open Source Lösung. Mit dem ausgewählten Tool wollen wir spezifische Logdateien analysieren und bewerten, damit wir demnächst potenzielle Angriffe erkennen können. Die Angriffserkennung soll automatisch mit der Eingabe von vordefinierten Regeln der Mitre ATT&CK® Matrix stattfinden.

=====

Unser Ziel ist eine umfangreiche Open Source Lösung zu finden bzw. geslatten, die uns ermöglichen, Cyberangriffe schnell und einfach zu detektieren. Proprietary Lösungen gibt es viele auf dem Markt, sie kosten meisten sehr viel und verlangen spezielle Kennt-

nis für die Verwaltung. Da solche Lösungen eher an großen Unternehmen eingeschränkt sind, beschäftigen wir uns mit dem Aufbau und Strukturierung unserer eigenen Lösung

=====

Diese Arbeit wird in folgende Teile geteilt:

- Definition von SIEMs und Log Analysis Tools
- Beschreibung von existierenden Proprietary und Open Source Lösungen
- Entscheidung für die Implementation einer Open Source Lösung
- Installation und Konfiguration von der ausgewählten Anwendung
- Definition von zwei spezifischen Cyberangriffen
- Festlegung von Regeln oder Use Cases für die automatische Erkennung von der vorherigen definierten Angriffen anhand der Mitre ATT&CK® Matrix
- Empfang, Bearbeitung und Eingabe in der ausgewählten Lösung der spezifischen Logdateien der Hochschule

Das folgende Diagramm stellt den Aufbau dieser Arbeit dar:

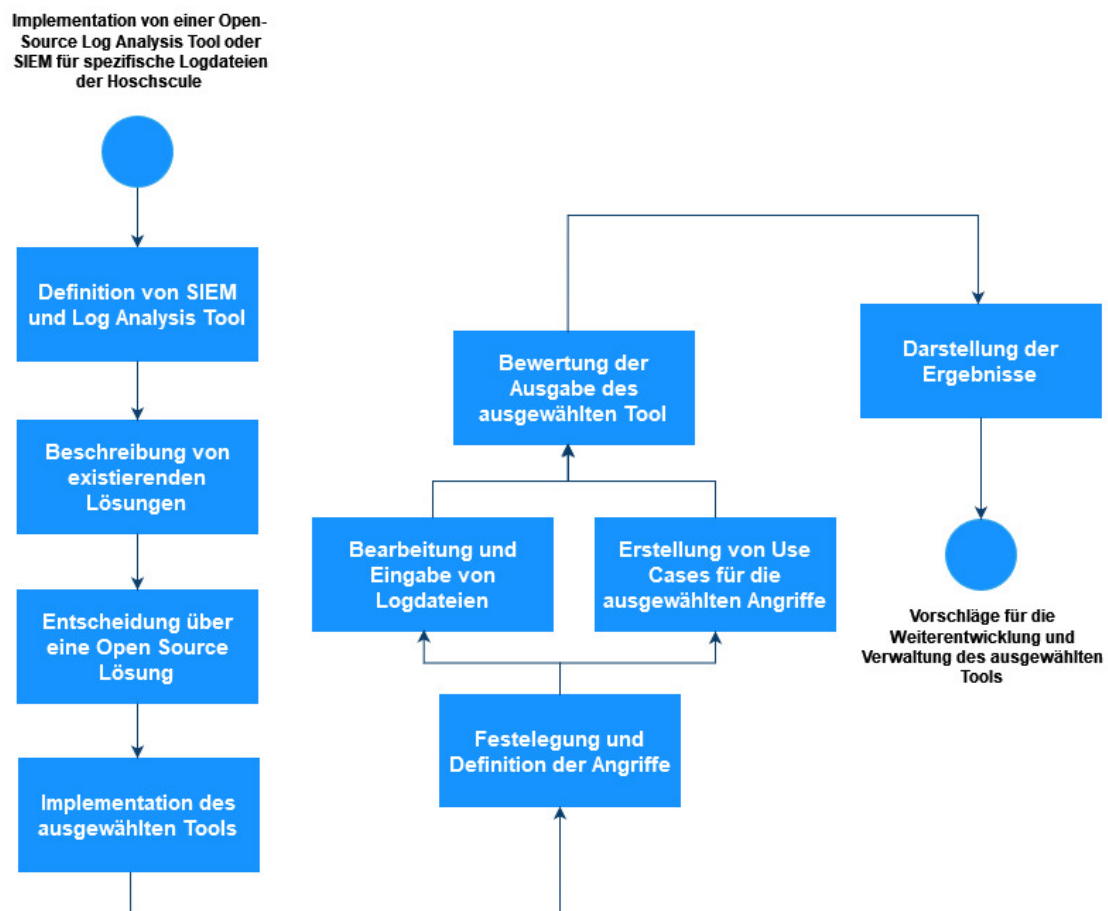


Abbildung 1: Aufbau dieser wissenschaftlichen Recherche SIEM  
Quelle: Eigene Darstellung

## 1.1 Problemstellung

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

- Wie können wir ein Log Analysis Tool so konfigurieren, dass es vordefinierten Angriffe nach der Mitre ATT&CK® Matrix automatisch erkennen kann?
- Wie können wir eine allgemeine Uses Cases definieren, sodass wir sie später für verschiedene Angriffsmuster nach Mitre ATT&CK® Matrix leicht anpassen können?

## 1.2 Vorgehensweise

Um diese oben genannten Ziele zu erreichen, verwenden wir folgenden Methoden:

- Recherche in der Fachliteratur über SIEMs und Log Analysis Tools Lösungen
- Vergleich zwischen verschiedenen Open Source und Proprietary Lösungen
- Installation von dem ausgewählten Tool
- Importieren von Logdateien in der ausgewählten Lösung
- Definition der Use Cases für die Angriffe



## 2 Definition von SIEMs und Log Analysis Tools

SIEM ist das Ergebnis einer Kombination zwischen dem Security Event Management (SEM) und Security Information Management (SIM) (Dorigo, 2012). Das Erste bezieht sich auf die Identifizierung, Bewertung, Beobachtung und Bericht von Sicherheitsvorfällen mithilfe von verschiedenen Log Dateien (techopedia, 2015). Das Zweite ist eine Software, die bei der automatischen Sammlung von Loginformationen aus vielen Quellen, wie Firewall und Servers unterstützt (techopedia, 2022). Da die meisten SIEM-Lösungen kostenpflichtig sind, existieren auch viele Open Source Log Analysis Tools, die eine ähnliche Aufgabe erledigen, ohne die Kernelementen von SIEM zu besitzen.

Log Analysis Tools sind meistens Anwendungen die Logdateien empfangen, speichern, bearbeiten und nach spezifischen eingegebenen Regeln bewerten. Diese Tools unterstützen Programmierer und Systemadministratoren bei der Überwachung des Zustands Systemen oder Software. Ein solches Tools kann Logdateien von verschiedenen Endpoints und mit verschiedenen Formattierungen bekommen und editieren, so dass es schließlich ein Bericht oder Graphik erzeugt (Łukasz Korzeniowski and Goczyla, 2022). Die Nutzung dieser Tools schränkt sich nicht in dem Sicherheitsbereich ein, sondern kann für das gesamte Rechenzentren nützlich sein.

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

Intrusion Detection System (IDS) sind Software oder Hardware, die Cyberangriffe identifizieren und berichten. Sie haben eine passive Rolle, da sie die Cyberangriffe weder stoppen noch verhindern können. Intrusion Prevention System (IPS) allerdings haben eine aktive Haltung gegenüber Cyberangriffe - die können automatisch behandeln können, indem sie Blocking-Mechanismen einschalten, um den Angriff zu stoppen (Wendzel, 2018). Wie das Intrusion Detection System (IDS), kann das Intrusion Prevention System (IPS) auch Logdateien generieren, die von einer SIEM-Lösung gesammelt werden können. SIEMs können seinerseits die Logdateien von diesen und von anderen Endpoints bekommen und diese nach vordefinierten Regeln bewerten, um dem SOC-Team über Sicherheitsvorfälle zu informieren oder automatisch Maßnahmen zu ergreifen. Wie SIEMs bekommen Log Analysis Tools auch Logdateien, um Bericht oder Darstellung zu generieren. Ihre Nutzung ist aber nicht so spezifisch wie die von SIEMs.

Die folgende Abbildung stellt didaktisch eine allgemeine Struktur von SIEM-Lösungen dar:

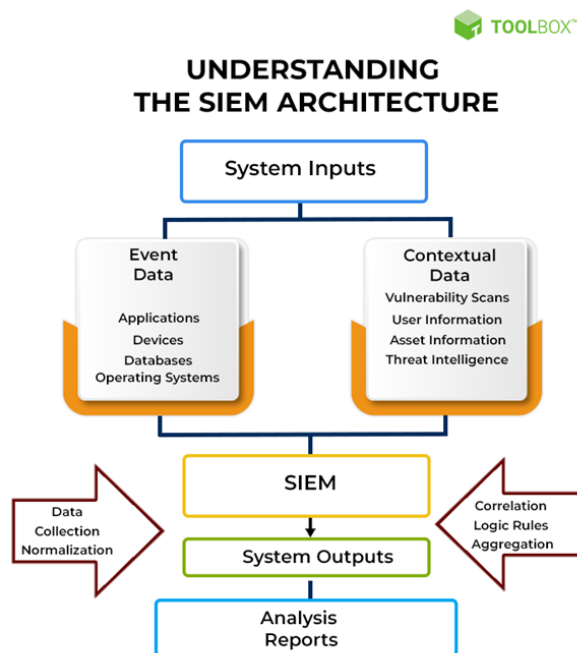


Abbildung 2: Allgemeine Struktur von SIEM  
Quelle: (Mohan, 2022)

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 wieder in der folgenden Abbildung darstellen werden:



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

Die folgende Abbildung stellt eine allgemeine Architektur von Log Analysis Tools dar:



Abbildung 4: Allgemeine Struktur von Log Analysis Tools  
Quelle: (Tek-Tools, 2020)

Den Informationsfluss eines Log Analyst Tools bildet folgendes Bild ab:

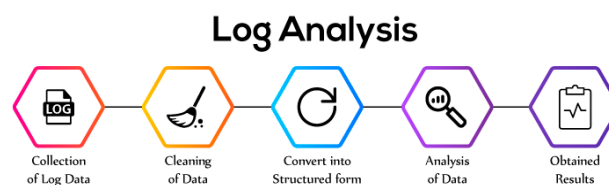


Abbildung 5: Allgemeine Informationsfluss von Log Analysis Tools  
Quelle: (neptune, 2023)

Aus bisheriger Beschreibung stellen wir fest, dass SIEM viel mehr als eine Sammlung von Logdateien sind. Das Ziel dieser Software ist die automatische Analyse zu ermöglichen, indem Daten kombiniert und bewertet werden können. In vielen Bereichen, wie Finanzen (Payment Card Industry Data Security Standard (PCDI DSS)), Gesundheitswesen (Health Insurance Portability and Accountability Act (HIPAA)), sind SIEMs eine gesetzliche Verpflichtung (Jog, 2020). In Deutschland verpflichtet das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme Organisationen mit kritischen Infrastrukturen die Anwendungen solcher Lösungen, um Störungen der Confidentiality, Integrity and Availability (CIA) zu verhindern (BSI, 2021). Log Analysis Tools sind seinerseits allgemeine Tools zu der Speicherung, Anpassung, Bewertung und Darstellung von Logdateien, ohne dass sie sich auf der Sicherheitsebenen fokussieren.

## 2.1 Existierende SIEMs Lösungen und Log Analysis Tools

Die existierenden SIEMs und Log Analysis Tools können in zwei Kategorien getrennt werden: *Proprietary* und *Open Source*. In folgenden Abschnitten präsentieren wir die proprietäre SIEM Splunk, um einen Maßstab für unsere Auswahl zu definieren, wenn es um Funktionalitäten geht. Wir analysieren folgende SIEMs und Log Analysis Tools:

- Prelude
- AlienVault Open Source Security Information Management (OSSIM)
- FortiSIEM
- ELK-Stack
- Grafana

### 2.1.1 Splunk

Splunk von dem Unternehmen Splunk Technology wurde 2003 in den USA veröffentlicht (Splunk, 2022b). Er gehört weltweit zu der meistverwendeten SIEM-Softwares und gilt als *State of the art* für andere ähnliche Lösungen (Kazarov et al., 2018). Zu ihren Kunden gehören große Konzerne wie Airbus, Coca-Cola, Intel und Deutsche Bahn.

Splunk bietet laut seiner Webseite folgenden Funktionalitäten an (Splunk, 2015):

- Skalierbare Datenplattform
- Risk-based Warnmeldung
- Bedrohungserkennung mithilfe von Machine Learning (ML)
- Automatische Aktualisierung von der Bedrohungs- und Schwachstelle-Database
- Unkomplizierte Installation und Anwendung

Die allgemeine Architektur und der Informationsfluss von Splunk unterscheiden sich nicht von den obigen dargestellten Struktur 2, Seite 17, und Informationsfluss3, Seite 18. Da es sich hier um eine proprietäre Lösung handelt, lässt sich Splunk mit vielen anderen Funktionalitäten verwalten und erweitern.

In Splunk funktioniert die Bedrohungserkennung mithilfe von Uses Cases. Laut der Dokumentation existieren sie in folgenden Szenarien: Überwachung, Untersuchung und Erkennung. Die Software ist sowohl mit glsmitre Matrix als auch mit Cyber Kill Chain (CKC®) für die Gestaltung ihrer Uses Cases integriert (Splunk, 2022a).

In einer spezifischen Arbeit wurden Angriffe auf einem System simuliert und schließlich mit Splunk analysiert, um Gefahren zu identifizieren und diese im Voraus zu sehen (Su et al., 2016). In anderer Arbeit beschrieben die Autoren, wie eine Splunk-Instanz installiert und konfiguriert wurden, um spezifische Brute-Force Angriffe zu erkennen (Selvaganesh et al., 2022).

### 2.1.2 Prelude

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

- Informationszentralisierung
- Datenaggregation und -Zusammenhang mit vordefinierten und von dem Nutzer angepassten Regeln
- Einbruchserkennungsmechanismen
- Datennormalisierung

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

Die folgende Abbildung zeigt die Integration verschiedener Module von Prelude und wie sie mit einander kommunizieren, um Analyse, Meldung und Speicherung zu generieren:



Abbildung 6: Integration zwischen den Modulen von Prelude

Quelle: (Prelude Team, 2007)

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

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

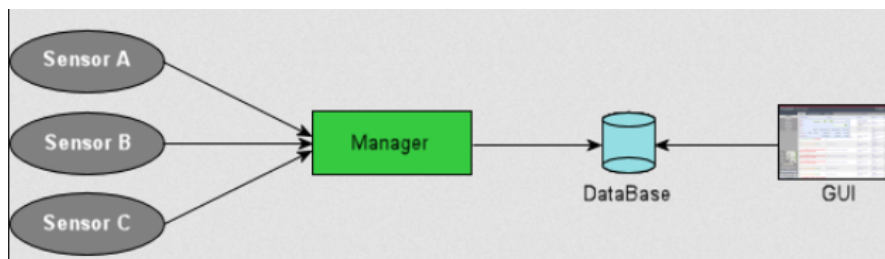


Abbildung 7: Einfache Architektur von Prelude  
Quelle: (Prelude Team, 2007)

In einer dezentralisierten Umgebung werden Daten von verschiedenen und getrennten Quellen generiert und bearbeitet. schließlich können die Nutzer auf diesen Daten unter einem Graphical user interface (GUI) zugreifen.



Abbildung 8: 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 nutzerfreundlicher 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 technischen Kriterien lag Prelude auf dem dritten Platz und in den benutzerfreundlichen Kriterien bekam Prelude den ersten.



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

### **2.1.3 AlienVault OSSIM**

AlienVault OSSIM ist eine im Jahr 2007 entwickelte Open Source SIEM Lösung. Im Jahr 2018 wurden sie von der Firma AT&T Communication gekauft (CBNINSIGHTS, 2020). In der Beschreibung des Anbieters steht, dass er sie auch dabei unterstützt, Daten zu sammeln, zu normalisieren und zu bewerten. Er behauptet auch, dass sein Tool in der Lage ist, Schwachstellen und Angriffe zu erkennen, das Verhältnis zu beobachten und Datenzusammenhang zu erschließen (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, da viele Funktionalitäten von der anderen Version stammen (AT&T Cybersecurity, 2022).

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



Abbildung 9: Architekturdiagramm 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 zu dem Tool einen IDS, ein Verhaltensüberwachungssystem und einen Schwachstellen-Scanner integriert sind. Die Anwendung ist auch mit der Plattform Open Threat Exchange(OTX) verbunden - diese ermöglicht eine Teilung von Informationen über die Schwachstelle. Comparitech highlighted, dass die Anwendung wegen ihrer niedrigen Kosten besser für kleine oder mittelständische Unternehmen geeignet ist (comparitech, 2023).

Die Anwendung soll konsistenten Daten Zusammenhang anbieten und soll das Auftauchen 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 wissenschaftlichen Quelle fanden wir heraus, dass für viele Quellen eine manuelle Normalisierung der Logdateien notwendig ist (Nabil et al., 2017). Die Anwendung hat aber einen zuverlässigen Berichtsmechanismus.

Während unserer Recherche gab es wenig wissenschaftliche Literatur, die sich um AlienVault OSSIM kümmert. Die meisten Publikationen waren aus kommerziellen Quellen und diese konzentrierten sich auf eine kostenpflichtige SIEM-Lösung von AT&T..

#### 2.1.4 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 benannte 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 (ML) integriert, sodass die Anwendung auch Verhältnisanalyse durchführen kann (Fortinet, 2022). Das Tool bietet auch eine umfangreiche und ausführliche Dokumentation an. Die nächste Abbildung zeigt die skalierbare Architektur des Tools:

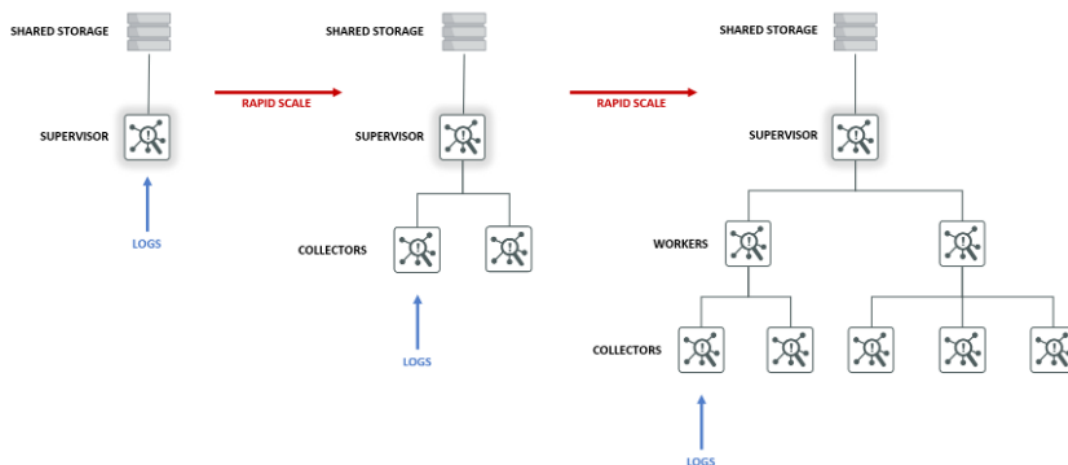


Abbildung 10: Skalierbare Architektur von FortiSIEM  
Quelle: (Fortinet, 2020)

Auch zu dieser SIEM-Lösung ist die wissenschaftliche Produktion eingeschränkt. Eine von der gefundenen Publikation betont, dass FortiSIEM eine schnelle Erkennung von Angriffen anbietet und über Network Operations Center (NOC) Funktionalitäten verfügt (Ramírez Tomás, 2018). Wie andere SIEMs Lösungen, hat FortiSIEM folgende Funktionalitäten:

- Datensammlung und Normalisierung
- Daten Zusammenhang
- Generierung von Berichten
- Warnmeldungen
- Datenauswertung

#### **2.1.5 ELK-Stack**

ELK Stack stammt aus der Verbindung von drei ursprünglichen Open Source Tools: Elasticsearch, Logstash und Kibana. Das Erste ist eine Such-und Analyse-Maschine. Das Zweite ist eine serverseitige Anwendung zur Datenverarbeitung und -Weiterleitung. schließlich Kibana ist dafür zuständig, visuelle Darstellung in Grafik-Format auszugeben (packt, 2019). Dieses Tool besitzt viele Eigenschaften einer SIEM-Lösung und wird von vielen SOC verwendet, ist aber, für viele Experten, kein SIEM für sich, da es über keine Warnmeldungssystem, Daten Zusammenhang und Vorfälleverwaltung verfügt (Miller, 2021). Diese und anderen Funktionalitäten lassen sich aber durch Plugins integrieren.

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

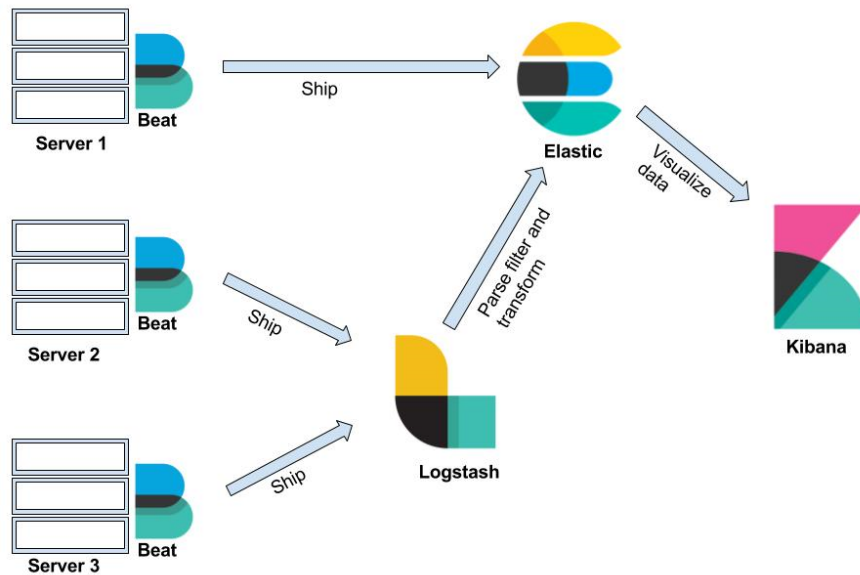


Abbildung 11: Integration zwischen Elasticsearch, Logstash und Kibana  
Quelle: (packt, 2019)

Die Beats auf dem Bild sind an der Endpoints installiert und leiten Daten entweder zu Elasticsearch oder zu Logstash weiter, wo sie schließlich bearbeitet werden (Jain, 2018).

Ein Teil der wissenschaftlichen Literatur zeigt die Log Analyse-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 (Wang et al., 2019).

Die offizielle Dokumentation von ELK Stack betont, dass die Anwendung folgende Funktionalitäten besitzt (elastic, 2022):

- Datensuche, -Normalisierung, -Analyse und
- Speicherung

- visuelle Ausgabe

Folgendes Diagramm aus der offiziellen Dokumentation zeigt die Aufteilung der Funktionalitäten pro Element von ELK Stack:

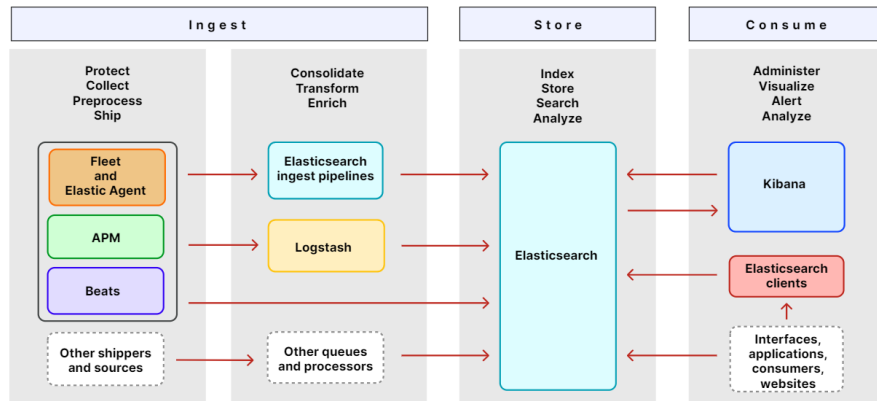


Abbildung 12: Aufteilung der Funktionalitäten zwischen den Komponenten  
Quelle: (elastic, 2022)

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

### 2.1.6 Grafana

Von allen recherchierten Lösungen ist Grafana die Einzige, die nicht als SIEM dargestellt ist. Grafana wird aber als Plattform für Visualisierung von Data beschrieben. Mit dem Tool ist es möglich eine Graphik zu erstellen und Meldungen zu definieren. Das Ziel der Anwendung ist, Information in einer einfachen und verständlichen Art und Weise zur Verfügung zu stehen (redhat, 2022).

Im Jahr 2014 wurde Grafana von der Firma Grafana Labs veröffentlicht. Das Tool basiert auf Kibana3,2.1.5. Ursprünglich sollte Grafana ein einfacheres Editingtool für Graphik sein und ermöglichen, Datenanfragen unkomplizierter zu machen. Die neueste Version,

9.4.3. wurde im März 2023 veröffentlicht und bietet viele Funktionalitäten an. Es ist auch möglich das Tool mithilfe von Plugins zu erweitern (Ödegaard, 2019)..

In der Webseite betont der Anbieter, dass Grafana die Zentralisierung und Zugang von Daten vereinfachen. Alle Art von Daten lassen sich analysieren und darstellen, von der Leistung von Anwendungen bis Verkaufsdaten und Krankheitsfällen. Die Anwendung soll auch den Zusammenhang von Daten ermöglichen, um wichtige Informationen herauszunehmen (Grafana Labs, 2016).

Grafana ist auch mit dem Logging Tool Loki integriert, sodass sich Logdateien aus unterschiedlichen Quellen integrieren lassen. Auf dem Folgenden Bild wird die Struktur von Grafana für Logging dargestellt:

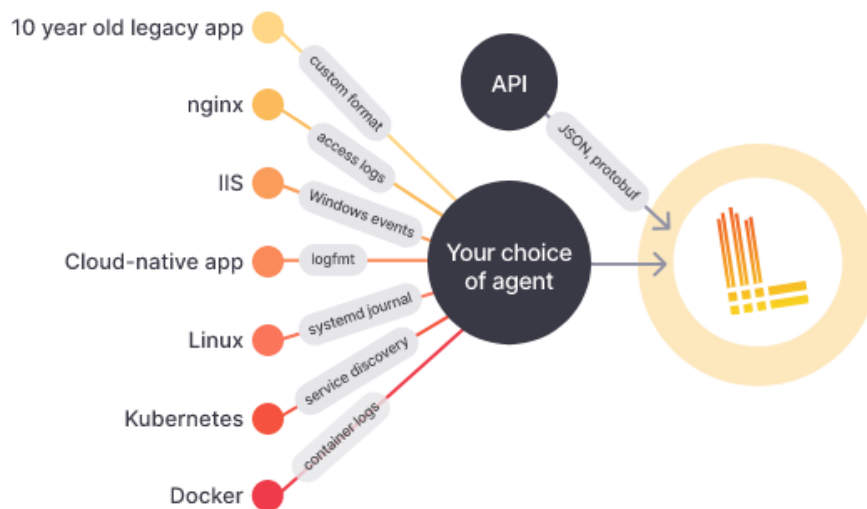


Abbildung 13: Integration von verschiedenen Log-Quellen mit Grafana Loki  
Quelle: (Grafana Labs, 2022)

Das Tool hat auch eine umfangreiche Dokumentation, die ausführlich erklärt, wie sie sich installieren, bedienen und mit anderen Tools integrieren lässt.

Obwohl Grafana nicht spezifisch für den Sicherheitsbereich konzipiert wurde, kann das Tool so eingerichtet werden, dass spezifische Logdateien gesammelt, bearbeitet und analysiert werden. Die Warnmeldung lässt sich mit Regeln oder Filter definieren. In einer Recherche von 2022 wurde Grafana dafür benutzt, Daten aus Netzwerkverkehr mithilfe von Grafana graphisch darzustellen (Manases and Zinca, 2022).

## ===== Literatur =====

Die Literaturrecherche über Grafana konzentriert sich eher auf die Anwendung des Tools auf spezifischen Kontexten, z.B. Überwachung von Cloud-Based Systemen, von Netzwerkaktivitäten und Netzwerkverkehr. In dieser Hinsicht gibt es wenige Recherche, wo das Tool, seine Implementierung und Integration mit anderen Tools die Hauptfigur ist.

## ===== Literatur =====

### 2.2 Auswahlkriterien

Eine umfangreiche SIEM Software die viele automatische Lösung für die Erkennung und Bekämpfung von Cyberangriffe würde perfekt für jede Situation passen. Da solche Lösungen meistens (oder alle) Proprietary sind und nur für teure Preise angeboten werden, entschieden wir uns für die Anpassung an einem Open SourceTool, das zu unserem Kontext und Einschränkungen gehört.

Demnächst beschäftigen wir uns mit Grafana. Wir beschreiben, wie wir das Tool installieren, konfigurieren und mit verschiedenen Logdateien eingeben. Nachdem die Grundfunktionalitäten eingerichtet sind und einwandfrei funktionieren, generieren wir anhand der Mitre ATT&CK® Matrix Uses Cases für die zukünftigen ausgewählten Angriffe. Unser Ziel ist Grafana so einzustellen, dass es in der Lage ist, die Muster dieser Angriffe zu erkennen und darüber zu berichten.



### 3 Implementation

In diesem Kapitel beschäftigen wir uns mit der Implementation und mit dem Aufbau von Grafana, sodass wir Cyberangriff nach dem Mitre ATT&CK® Matrix erkennen können. Wir gestalten unser Arbeitslabor mit Container und virtuellen Maschine (VM), wie in dem folgenden Diagramm:

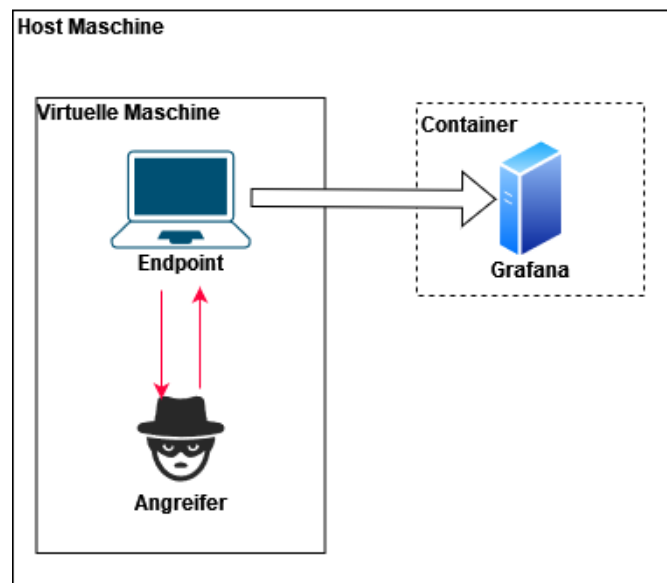


Abbildung 14: Aufbau unseres Arbeitslabors  
Quelle: Eigene Quelle

Von unserem Aufbau zielen wir, die Aufnahmen und Anpassung der Logdateien für Grafana, die Mustererkennung für die ausgewählten Cyberangriffe und schließlich die Warnmeldung für die Endnutzer, sodass sie sich für entsprechende Sicherheitsmaßnahmen entscheiden können. Dieser Ablauf ist in dem folgenden Diagramm dargestellt:

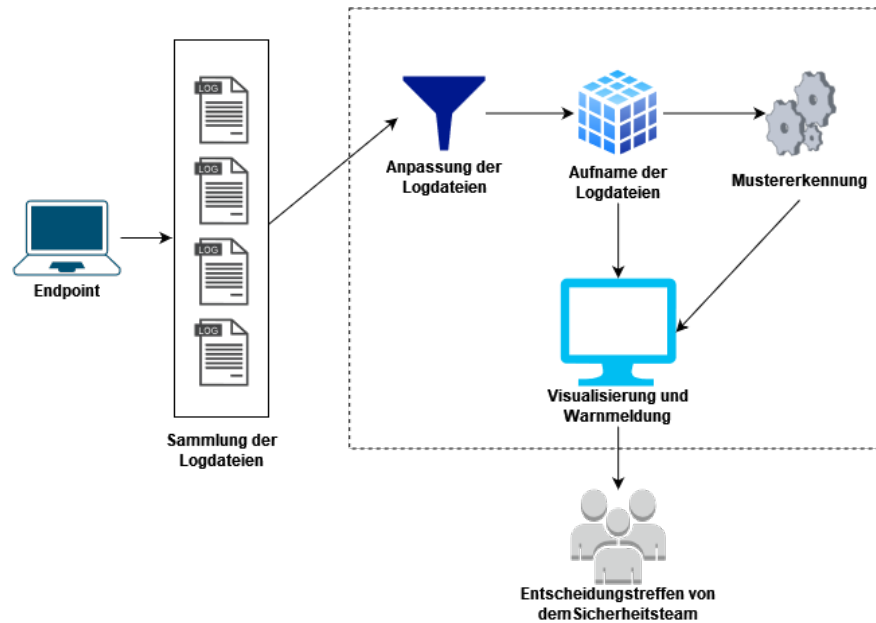


Abbildung 15: Erwarteter Ablauf von der Datensammlung bis zur Warnmeldung von Cyberangriffen  
 Quelle: Eigene Quelle

### 3.1 Angriffserkennung mithilfe von Mitre ATT&CK Matrix®

Es gibt verschiedene Methode und Framework zur Vermeidung, Erkennung, und Unterbrechung von Cyberangriffen. Open Web Application Security Project®(OWASP®), Cyber Kill Chain (CKC®) und Mitre ATT&CK® Matrix sind einige Beispiele von denen, die SOC-Teams verwenden, um Sicherheit von Systemen und/oder Netzwerken zu gewährleisten. Da die Richtlinien und Fokus von diesen Frameworks sich unterscheiden können und deswegen anderen Aufbau von unserer Struktur verlangen wurden, entschieden wir uns für die Anwendung von der Mitre ATT&CK® Matrix für die Erkennung der Cyberangriffe besonders, weil dieser Framework auch an Splunk integriert ist.

Die Mitre ATT&CK® Matrix hat folgende Hauptnutzung (MITRE ATT&CK, 2018b):

- Erkennung und Analyse von Angriffstechnik
- strukturierte Datensammlung über Bedrohungen
- Emulieren von Cyberangriffe für die Anwendung an Angriffssübungen
- Systemhärtung und Verbesserung der Verteidigungsmaßnahmen

Die Matrix bietet eine umfangreiche Verwendung für Unternehmen und für SOC-Team an, um ihre wertvollen Resource schützen und ihre Fachkenntnisse über Cybersicherheit zu erweitern (Hazel, 2021). Hier konzentrieren wir uns auf die Entwicklung und auf die Implementierung einer Methode für die automatische Erkennung und Analyse von Angriffstechnique in Grafana.

Die Mitre ATT&CK® Framework besteht aus 14 Taktik. Zu jedem Taktik gehören Technique, die ihrerseits in Subtechniques aufgeteilt sind. Jede Subtechnique wird mit Beispielen, Härtungsmaßnahmen und Erkennungsregeln dargestellt. Die Folgebende Abbildung zeigt, wie diese Struktur aufgebaut ist:

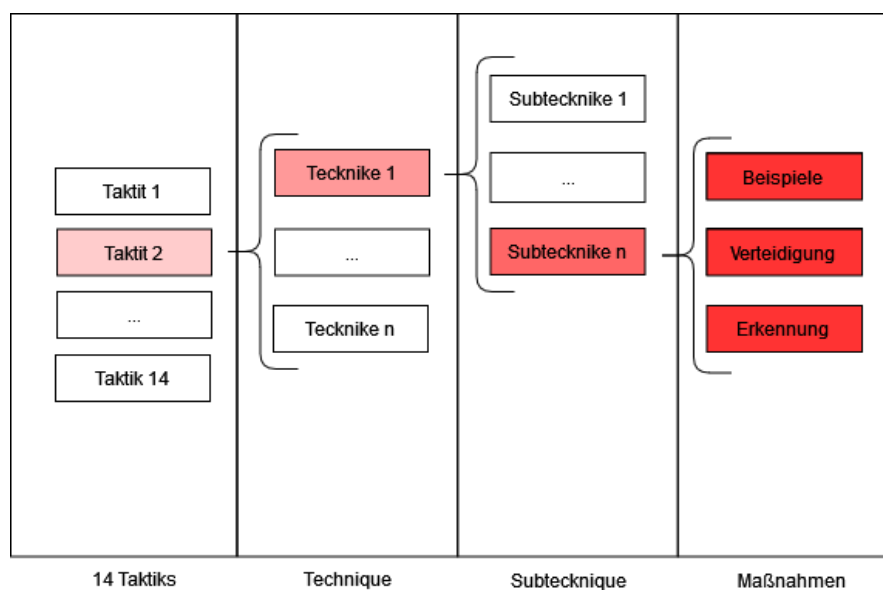


Abbildung 16: Struktur der Mitre Matrix Cyberangriffe  
Quelle: Eigene Quelle

Die 14 Tactics sind folgende:

- Informationssammlung für zukünftige Angriffe
- Entwicklung von Ressource von Angreifer
- Erster Zugang zum Opfersysteme
- Ausführung von böartigen Coden
- Beharrlichkeit von System
- Privilegienausweitung
- Vermeidung von Verteidigungssysteme
- Zugang zu Anmeldedaten
- Umgebungserkennung
- Seitliche Bewegung zu anderem Systemen innerhalb des Angriffsziels
- internet Informationssammlung
- Steuerung und Kontrolle (C2 - Command and Control im Original)
- Datenextrahierung
- Auswirkung auf die Integrität

In dieser Arbeit beschäftigen wir uns mit Tactic SZugang zu Anmeldedaten und deren Technique Brute-Force Angriffe. Diese Technique ist in vier Subtechnique aufteilt

- Erraten von Anmeldedaten
- Entschlüsselung von Hashwerte
- *Password Spraying*
- *Password Stuffing*

Um den Umfang dieser Arbeit an ihren Einschränkungen anzupassen, lassen wir unseren Fokus auf die Erkennung der Subtechnique Erraten von Anmeldedaten und *Password Stuffing*, da diese Angriffe ähnliche Erkennungsmethode haben. Hier schließen wir auch die anderen Maßnahmen aus.

Die nächste Abbildung zeigt den Umfang unseres Implementationsversuchs:

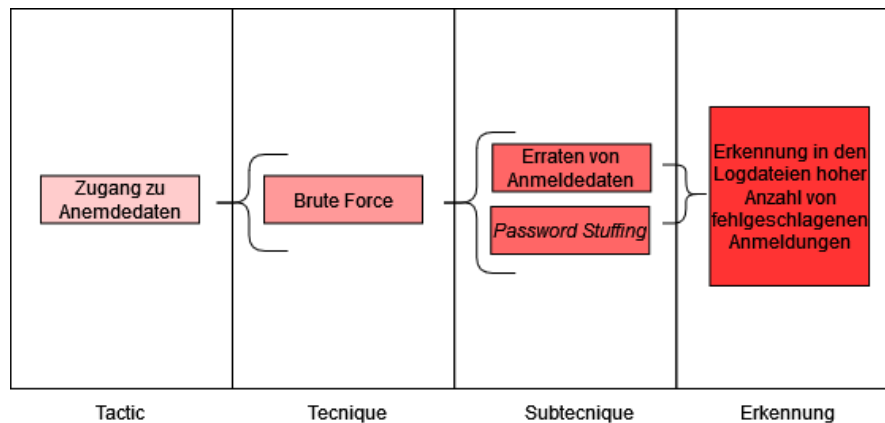


Abbildung 17: Analysestruktur für diese Arbeit Cyberangriffe  
Quelle: Eigene Quelle und (MITRE ATT&CK, 2020)

### 3.2 Aufbau der Erkennungsregel für den ausgewählten Angriff

Der Brute-Force Angriffe lässt sich durch die Anzahl des fehlgeschlagen Anmeldeversuchs erkennen (Selvaganesh et al., 2022). Wir bearbeiten eine Situation, in der es keine Gegenmaßnahmen, wie Kontosperre nach  $n$  beliebigen Versuchen oder MFA, implementiert sind. Das folgende Aktivitätsdiagramm stellt einen allgemeinen Ablauf eines Anmeldeverfahrens dar:

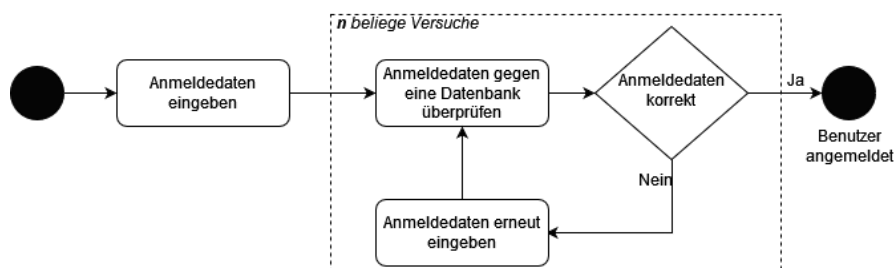


Abbildung 18: Allgemeiner Ablauf eines Anmeldeverfahrens  
Quelle: Eigene Quelle und (Selvaganesh et al., 2022)

### **3.3 Bewertung der Daten in Grafana**

Hinzufügen der Logdateien und Erstellung von Regeln zur Erkennung des Angriffes Diagramm der Nutzung von Grafana

### **3.4 Normalisierung der Logdateien mit Zeek**

Diagramm der Nutzung von Grafana und Zeek

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

- Implementation in Container

### **3.5 Sammlung von Server-Log Dateien**

### **3.6 Normalisierung der Log-Dateien**

## **4 Fazit**

Zusammenfassung von

- Zielen
- Ergebnissen
- 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 07.03.2023.
- AT&T Cybersecurity (2022). Alienvault ossim.  
<https://cybersecurity.att.com/products/ossim>. Zugriff am 05.03.2023.
- Ba, M. H. N., Bennett, J., Gallagher, M., and Bhunia, S. (2021). A case study of credential stuffing attack: Canva data breach. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 735–740.  
<https://doi.org/10.1109/CSCI54926.2021.00187>. Zugriff am 26.03.2023.
- 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 04.03.2023.
- CBNINSIGHTS (2020). Alienvault.  
<https://www.cbinsights.com/company/alienvault>. Zugriff am 05.03.2023.
- Centers for Disease Control and Prevention (2016). Health Insurance Portability and Accountability Act of 1996 (HIPAA).  
<https://www.pcicomplianceguide.org/faq/>. Zugriff am 04.03.2023.
- comparitech (2023). The Best SIEM Tools for 2023 Vendors & Solutions Ranked.  
<https://www.comparitech.com/net-admin/siem-tools/>. Zugriff am 05.03.2023.
- 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 03.03.2023.
- Douglis, F. and Nieh, J. (2019). Microservices and containers. *IEEE Internet Computing*, 23(6):5–6.  
<https://doi.org/10.1109/MIC.2019.2955784>. Zugriff am 23.03.2023.
- elastic (2022). *Elastic Docs*.  
<https://www.elastic.co/guide/en/welcome-to-elastic/current/new.html>. Zugriff am 5.02.2023.
- European Commission (2015). Siem design and development.  
<https://cordis.europa.eu/project/id/644425>. Zugriff am 05.03.2023.
- Fortinet (2016). Fortinet Announces Acquisition of AccelOps .  
<https://www.fortinet.com/corporate/about-us/newsroom/press-releases/20>



- 16/fortinet-announces-acquisition-of-accelops. Zugriff am 06.03.2023.
- Fortinet (2020). FortiSIEM Reference Architecture.  
[https://www.fortinet.com/content/dam/maindam/PUBLIC/02\\_MARKETING/02\\_Colateral/DeploymentGuide/dg-fortisiem-reference-architecture.pdf](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Colateral/DeploymentGuide/dg-fortisiem-reference-architecture.pdf). Zugriff am 06.03.2023.
- Fortinet (2022). FortiSIEM Solutions.  
<https://www.fortinet.com/products/siem/fortisiem>. Zugriff am 06.03.2023.
- 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 06.03.2023.
- Grafana Labs (2016). Dashboard anything. Observe everything.  
<https://grafana.com/grafana/>. Zugriff am 12.03.2023.
- Grafana Labs (2022). Dashboard anything. Observe everything.  
<https://grafana.com/logs/>. Zugriff am 12.03.2023.
- 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 21.02.2023.
- 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 am 03.03.2023.
- Hazel, T. (2021). How To Use the MITRE ATT&CK Framework.  
<https://www.chaossearch.io/blog/how-to-use-mitre-attck-framework>. Zugriff am 26.03.2023.
- Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., hoon jae lee, and Sain, M. (2019). Multi-Factor Authentication in Cyber Physical System: A State of Art Survey. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pages 279–284. <https://doi.org/10.23919/ICACT.2019.8701960>, Zugriff am 26.03.2023.
- IT-Service.Network (2020). Was ist ein plug-in?  
<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>. Zugriff am 04.03.2023.
- Jain, U. (2018). *Lateral Movement Detection Using ELK Stack*. PhD thesis, University of Houston.  
<https://uh-ir.tdl.org/handle/10657/3109>. Zugriff am 07.03.2023.
- Janiesch, C., Zschech, P., and Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, 31(3):685–695.

- <https://doi.org/10.1007/s12525-021-00475-2>. Zugriff am 13.03.2023.
- Jog, Y. (2020). Security Information and Event Management (SIEM).  
<https://www.linkedin.com/pulse/security-information-event-management-siem-yatin-jog>. Zugriff am 04.03.2023.
- 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 04.03.2023.
- Manases, L. and Zinca, D. (2022). Automation of network traffic monitoring using docker images of snort3, grafana and a custom api. In *2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pages 1–4.  
<https://doi.org/10.1109/RoEduNet57163.2022.9921063>. Zugriff am 13.03.2023.
- Martin, L. (2018). The cyber kill chain.  
<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. Zugriff am 12.03.2023.
- Microsoft Security (2022). Endpoints defined.  
<https://www.microsoft.com/en-us/security/business/security-101/what-is-an-endpoint>. Zugriff am 12.03.2023.
- 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 07.03.2023.
- MITRE ATT&CK (2018a). Frequently Asked Questions.  
<https://attack.mitre.org/resources/faq/>. Zugriff am 12.03.2023.
- MITRE ATT&CK (2018b). Getting Started.  
<https://attack.mitre.org/resources/getting-started/>. Zugriff am 26.03.2023.
- MITRE ATT&CK (2020). Brute Force.  
<https://attack.mitre.org/techniques/T1110/>. Zugriff am 26.03.2023.
- 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 20.02.2023.
- 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 26.02.2023.
- 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 26.02.2023.

- neptune (2023). A Machine Learning Approach to Log Analytics: How to Analyze Logs?  
<https://www.nexcess.net/blog/open-source-vs-proprietary/>. Zugriff am 12.03.2023.
- Nexcess (2022). Open source vs. proprietary: Which is better?  
<https://www.nexcess.net/blog/open-source-vs-proprietary/>. Zugriff am 26.02.2023.
- NIST (2020a). About nist.  
<https://www.nist.gov/about-nist>. Zugriff am 19.02.2023.
- NIST (2020b). Glossary.  
<https://csrc.nist.gov/glossary/>. Zugriff am 19.02.2023.
- 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/ch01lv11sec10/what-is-elk-stack>. Zugriff am 07.03.2023.
- Prelude SIEM (2018). Prelude SIEM: Smart Security.  
<https://www.prelude-siem.com/en/prelude-siem-en/>. Zugriff am 05.03.2023.
- Prelude SIEM (2020). *Prelude Documentation: version 5.2*.  
<https://www.prelude-siem.org/docs/5.2/en/>. Zugriff am 06.03.2023.
- Prelude Team (2007). *Manual User*.  
<https://www.prelude-siem.org/projects/prelude/wiki/>. Zugriff am 06.03.2023.
- 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., Giannakoulis, 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 am 03.03.2023.
- 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%20c3%adrez%20-%20Implementaci%20c3%b3n%20de%20un%20sistema%20de%20gesti%20c3%b3n%20de%20eventos%20de%20seguridad%20en%20una%20empresa%20de%20tama%20c3%b1...pdf?sequence=1&isAllowed=y>. Zugriff am 06.03.2023.
- redhat (2022). What is grafana?  
<https://www.redhat.com/en/topics/data-services/what-is-grafana>. Zugriff am 13.03.2023.
- Roser, M., Ritchie, H., and Ortiz-Ospina, E. (2015). Internet. *Our World in Data*.  
<https://ourworldindata.org/internet>. Zugriff am 17.02.2023.

- Savic, D., da Silva, A. R., Vljajic, S., Lazarevic, S., Stanojevic, V., Antovic, I., and Milic, M. (2012). Use case specification at different levels of abstraction. In *2012 Eighth International Conference on the Quality of Information and Communications Technology*, pages 187–192.  
<https://doi.org/10.1109/QUATIC.2012.64>. Zugriff am 12.03.2023.
- Selvaganesh, M., Karthi, P., Kumar, V. A. N., and Moorthy, S. R. P. (2022). Efficient brute-force handling methodology using indexed-cluster architecture of splunk. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, pages 697–701.  
<https://doi.org/10.1109/ICEARS53579.2022.9752323>. Zugriff am 12.03.2023.
- Sowmya, G. V., Jamuna, D., and Reddy, M. V. K. (2012). Blocking of Brute Force Attack. *International journal of engineering research and technology*, 1.
- Splunk (2015). Splunk Enterprise Security.  
[https://www.splunk.com/en\\_us/products/enterprise-security.html](https://www.splunk.com/en_us/products/enterprise-security.html). Zugriff am 12.03.2023.
- Splunk (2022a). Use Cases.  
<https://docs.splunk.com/Documentation/ES/7.1.0/Usecases/Overview>. Zugriff am 12.03.2023.
- Splunk (2022b). What Is Security Information and Event Management (SIEM)?  
[https://www.splunk.com/en\\_us/data-insider/what-is-siem.html](https://www.splunk.com/en_us/data-insider/what-is-siem.html). Zugriff am 12.03.2023.
- Su, T.-J., Wang, S.-M., Chen, Y.-F., and Liu, C.-L. (2016). Attack detection of distributed denial of service based on splunk. In *2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE)*, pages 397–400.  
<https://doi.org/10.1109/ICAMSE.2016.7840355>. Zugriff am 12.03.2023.
- Swathi, K. (2022). Brute Force Attack on Real World Passwords. *International Journal of Research Publication and Reviews*, 3(11):552–558.  
<https://www.ijrpr.com/archive.php?volume=3&issue=11>. Zugriff am 26.02.2023.
- Tanembaum, A. S. (2009). *Moderne Betriebssysteme*. Pearson, München.
- 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.
- Tek-Tools (2020). Log Analysis – How to Use a Log Analyzer Tool?  
<https://www.tek-tools.com/apm/choosing-log-analyzer-tool>. Zugriff am 12.03.2023.
- U.S. Department of Health & Human Services (2016). The HIPAA Privacy Rule.  
<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>. Zugriff am

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.
- 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](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.
- Ödegaard, T. (2019). The (Mostly) Complete History of Grafana UX.  
<https://grafana.com/blog/2019/09/03/the-mostly-complete-history-of-grafana-ux/>. Zugriff am 13.03.2023.
- Łukasz Korzeniowski and Goczyla, K. (2022). Landscape of automated log analysis: A systematic literature review and mapping study. *IEEE Access*, 10:21892–21913.  
<https://doi.org/10.1109/ACCESS.2022.3152549>. Zugriff am 12.03.2023.