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

Abstract

XXXXXXXXXXXXXXXXXXX

Abbildungsverzeichnis

Glossar

Brute-Force Angriffe Systematischer Versuch, Credentials oder andere sensitive Daten zu raten, indem verschiedenen Buchstaben, Ziffern und Symbolen kombiniert werden (Sowmya et al., 2012). 14

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 ihren Daten zu stehlen oder zu dominieren (NIST, 2020b). 7, 8, 11, 25

Confidentiality, Integrity and Availability (CIA) Beschreibt die drei wichtigsten Schutzziele der IT-Sicherheit: Vertraulichkeit, Integrität und Verfügbarkeit (Wendzel, 2018). 13

Cyber Kill Chain®(CKC®) Auch *Cyberattack Lifecycle* genannt, bezieht sich auf eine Sicherheitsmodell für die Identifizierung, Analysis und Unterbrechung von fortgeschrittene Cyberangriffe. Dieses Model hat sieben festgelegte Phasen: *Recoinnaissance*, *Weaponization*, *Delivery*, *Exploitation*, *Installation*, *Command & Control (C2)* und *Actions on Objectives* (Martin, 2018). 14

Endpoint Bezieht sich auf Geräte oder Systemen, die in der Netzwerk verbunden sind. Diese können z.B. Handys, Servers, Computers, Sensoren sein. (Microsoft Security, 2022). 10, 11, 22

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme ein im Jahr 2021 verabschiedetes Bundesgesetz zur Erhöhung von Sicherheit informationstechnischen Systemen besonders, solche von den kritischen Infrastrukturen (Harmes, 2023). 13

falsch positiv Eine aus einer fehlerhaften erkannten Verwundbarkeit Warnmeldung (NIST, 2020b). 19

Graphical user interface (GUI) eine Schnittstelle, die den Nutzer ermöglicht, mithilfe von Symbolen und visuellen Elementen mit der Anwendung zu interagieren (Fu, 2018). 16

Health Insurance Portability and Accountability Act (HIPAA) US-Bundesgesetz über den Schutz von sensitiven personenbezogenen Gesundheitsdaten (U.S. Department of Health & Human Services, 2016). 13

Machine Learning (ML) Bezieht sich auf die Fähigkeit von Systemen, automatisch Problem zu lösen und spezifische Aufgabe zu erledigen mithivel von Datenbeziehung und Bearbeitung (Janiesch et al., 2021). 14, 20

Mitre ATT&CK® Abkürzung für *Adversarial Tactics, Techniques and Common Knowledge*. Es beziehit sich auf eine weltweit zugängliche Wissensbasis mit detallierter Beschreibung, Klazifizuerung und Bekämpfung von verschiedenen Angriffstechnike (MITRE ATT&CK, 2018). 7–9, 14, 25

National Institute of Standards and Technology (NIST) US-Behörden, die für die Reglungen, Vereinheitlichung und Weiterentwicklung im Bereich Informationstechnologie zuständig sind (NIST, 2020a). 7

Open Source Beschreibt Code, die jeder zugreifen, modifizieren und verbreiten können, ohne dafür Lizenzen bezahlen zu müssen (Open Source Initiative, 2007). 7–10, 13, 15, 18, 21, 25

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). 13

Network Operations Center (NOC) Zentralisierter Bereich eines Unternehmens dafür zuständig, Netzwerkaktivitäten zu überwachen und zu verwalten (Mohammed et al., 2021). 21

Plugin Optionale Software-Komponenten, die weitere Funktionalitäten zu einer Anwendung hinzufügen (IT-Service.Network, 2020). 21, 23

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 originellen Code(Nexcess, 2022). 7, 9, 13, 25

Security Operations Center (SOC) Zentralisierter Bereich eines Unternehmens dafür zuständig, Sicherheitsvorfälle zu überwachen, zu identifizieren, zu bewerten und dazu zu reagieren (Vielberth, 2021). 7, 10

Use Cases Beschreiben die Interaktion zwischen Systemen und Benutzer. Sie dienen zu der Anforderungserhebung eines Systems (Savic et al., 2012). 8, 9, 14, 25

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.

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.

SIEM Security Information and Event Management.

SEM Security 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: Soziale Netzwerke, 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 viele Firmen das sogenannte Security Information and Event Management (SIEM) oder Log Analysis Tools.

Das National Institute of Standards and Technology (NIST) definiert SIEM als Software für die Sammlug, 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/or Löchen, Weiterleitung und Überwachung von Loginformationen. In dieser Arbeit benutzen wir den Begriff "Log Analysis Tool", um diese Systemen zu referenzieren

In diesem Projekt recherchieren und vergleichen wir existierende SIEM und Log Analysis Tools. Danach entscheiden wir uns für eine Open Source Lösung, sodass wir sie für spezifische Logdateien der Hochschule Worms anwenden können. Die Angriffserkennung soll automatisch mit der Eingabe von vordefinierten Regeln der Mitre ATT&CK® Matrix stattfinden.

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 Lösungen

- Installation und Konfiguration von der ausgewählten Anwendung
- Definition von zwei spezifischen Cyberangriffe
- Festelung von Regeln oder Use Cases für die automatische Erkennenung von der vorherigen definierten Angriffe Anhand der Mitre ATT&CK® Matrix
- Empfang, Bearbeitung und Eingabe in der ausgewählten Lösung der spezifischen Logdatein der Hochschule
- Analyse, Bewertung und Zukunft dieser Recherche

Das folgende Diagramm stellt den Aufbau dieser Arbeit dar:

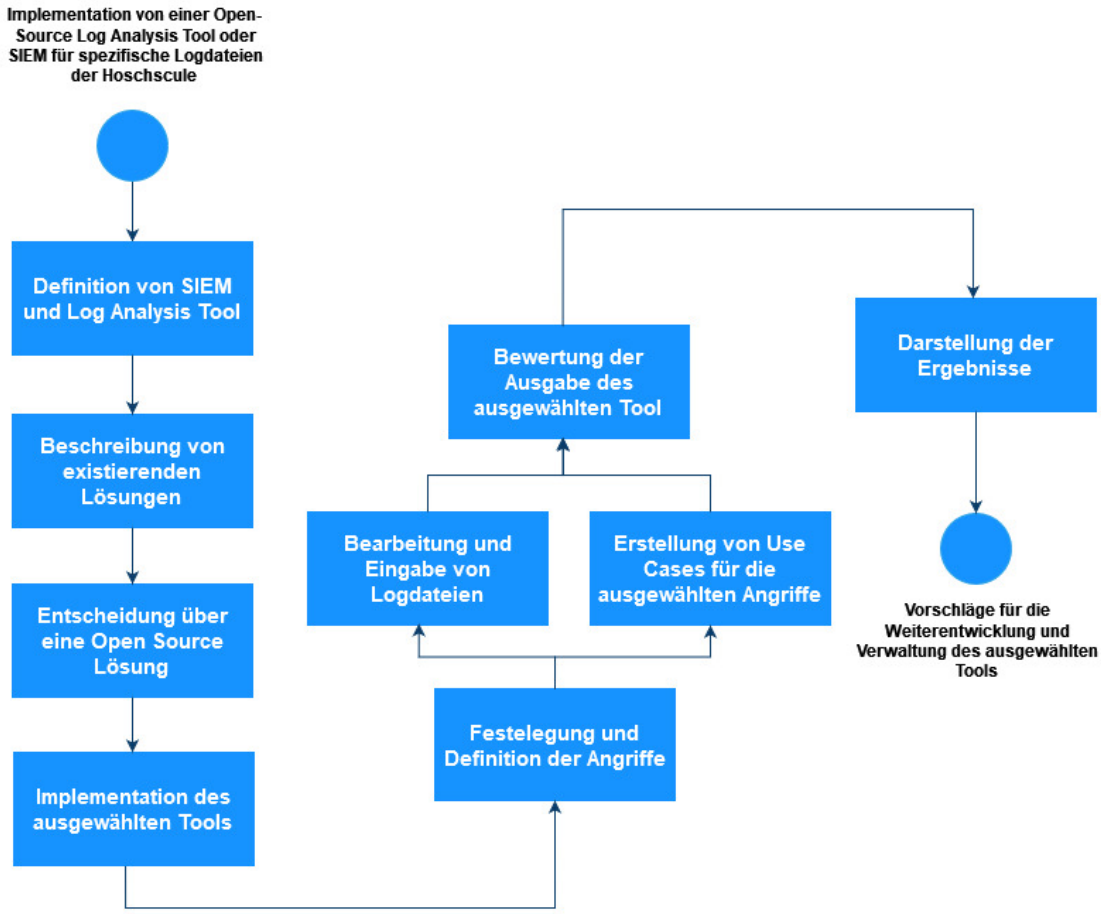

Abbildung 1: Aufbau dieser wissenschaftlichen Recherche SIEM
Quelle: Eigene Darstellung

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 Use Cases definieren, sodass wir sie später für verschiedene Angriffsmuster nach Mitre ATT&CK® Matrix leicht anpassen können?

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

1.2 Vorgehensweise

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

- Recherche in der Fachliteratur über SIEMs und Log Analysis Tools Lösungen
- Vergleich zwischen verschiedenen Open Source und Proprietary Lösungen
- Installation von der 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 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 Log Dateien (techopedia, 2015). Das zweite ist ein 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 spezifisichen eingegebenen Regeln bewerten. Diese Tools unterstützen Programmieren 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 Goczyła, 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 Aufgabe mehr Zusammenhang als Unterschied haben. Um den Umfang dieser Arbeit wegen der zeitlichen Einschränkungen zu verringern, fassen wir kurz die Unterschiede zwischen ihnen 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, weil sie die Cyberangriffen weder stoppen noch verhindern können. Intrusion Prevention System (IPS) seinerseits haben eine aktive Haltung gegenüber Cyberangriffe, die können automatisch behandeln können, indem sie Blocking-Mechanism 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 können. SIEMs können seinerseits die Logdateien von diesen und von anderen Endpoints bekommen und diese nach vordefierten Regeln bewerten, um dem SOC-Team über Sicherheitsvorfälle zu informieren oder automatisch Maßnahmen zu greifen. Wie SIEMs bekommen Log Analysis Tools auch Logdateien, um Bericht oder Darstellung zu genieren, ihre Nutzung ist aber nicht so spezifisch wie die von SIEMs.

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

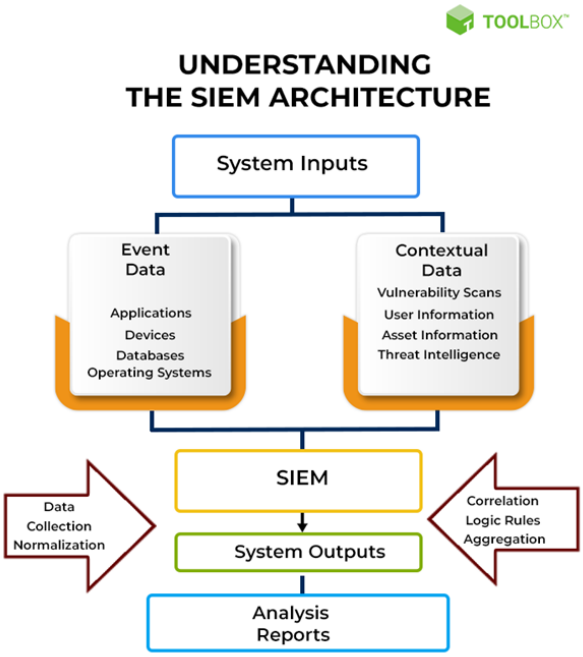

Abbildung 2: Allgemeine Struktur von SIEM
Quelle: (Mohanan, 2022)

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 wieder in der folgenden Abbildung darstellen:

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

Die folgenden Abbildung stellen eine allgemeine Architektur von Log Analysis Tools dar:

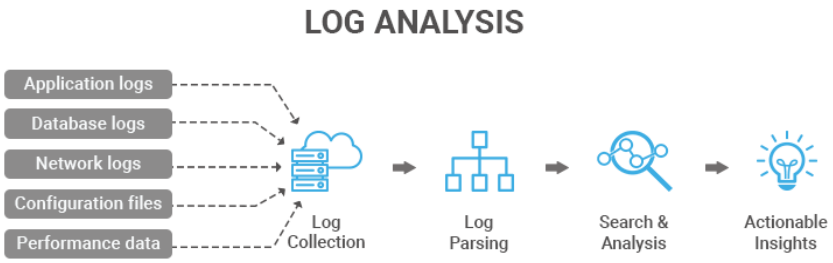

Abbildung 4: Allgemeine Struktur von Log Analysys Tools
Quelle: (Tek-Tools, 2020)

Den Informationsfluss eines Log Analysys Tools zeigen auf dem folgenden Bild:

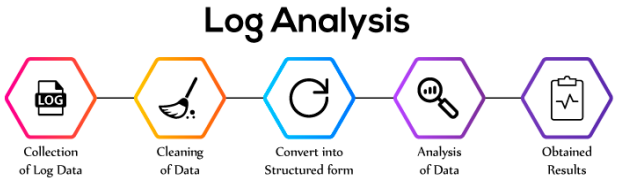

Abbildung 5: Allgemeine Informationsfluss von Log Analysys Tools
Quelle: (neptune, 2023)

Aus den bisherigen 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 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 (BSI, 2021). Log Analysis Tools sind seinerseits allgemeine Tools zu der Speicherung, Anpassadung, Bewertung und Darstellung von Logdateien, ohne dass sie 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 den folgenden Abschnitte präsentieren wir die proprietäre SIEM Splunk, um einen Maßtab für unsere Auswahl zu definieren, wenn es um Funktionalitäten geht. Wir analysieren folgenden 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 veröffentlich (Splunk, 2022b). Er gehört weltweit zu der meist verwendeten SIEM Software und gilt als *State of the art* für andere ähnliche Lösungen (Kazarov et al., 2018). Zu ihren Kunden gehören großen Konzerne wie Airbus, Coca-Cola, Intel und die Deutsche Bahn.

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

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

Die allgemeine Architektur und Informationsfluss von Splunk unterscheided sich nicht von den obigen dargestellten Struktur 2, Seite 13, und Informationsfluss 3, Seite 14. Da es sich hier um eine proprietäre Lösung geht, lässt sich Splunk mit vielen anderen Funktionaliäten 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 Mitre ATT&CK® als auch mit Cyber Kill Chain (CKC®) für die Gestaltung ihrer Uses Cases integriert (Splunk, 2022a).

In der wissenschaftlichen Literatur wird Splunk viel recherchiert. Verschiedene wissenschaftliche Arbeite beschäftigen sich mit der Integration und Nutzung dieser Anwendung. In einer spezifischen Arbeit wurden Angriffe auf einem System simuliert und schließlich mit Splunk analysiert, um Gefahren zu identifieren 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 gehört zu einer europäischen Open Source SIEM Lösung. Laut dem Anbieter verfügt Prelude unter anderen folgenden Funktionalitäten (Prelude SIEM, 2018):

- Informations Zentralisierung
- 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 zentralen 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:

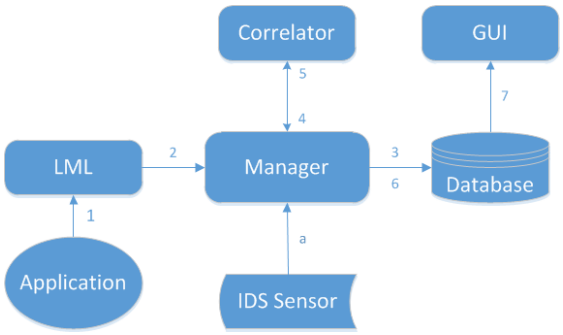

Abbildung 6: Integration zwischen den Modulen von Prelude
Quelle: (Prelude Team, 2007)

Aus der Abbildung und der Dokumentation können wir folgenden Informationsfluss: die Daten werden von Endanwendung generiert und zum Loganalyzer (Prelude Log Monitoring Lackey (LML)) geschickt, wo sie normalisiert und bewertet sind. Für solche Logs, wo es verdächtige Werte gibt, werden Warnmeldungen generiert. Diese Meldungen wirden zum Manager Module weitergeleitet. Der Correlator oben sucht nach Zusammenhang zwischen anderen Daten. Das Ergebnis von Correlator ist wieder zum Manager geschicht 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 zentralisierter als auch einen dezentralisierten Aufbau. In der nächsten Abbildung sehen wir eine einfache Implementation von Prelude:

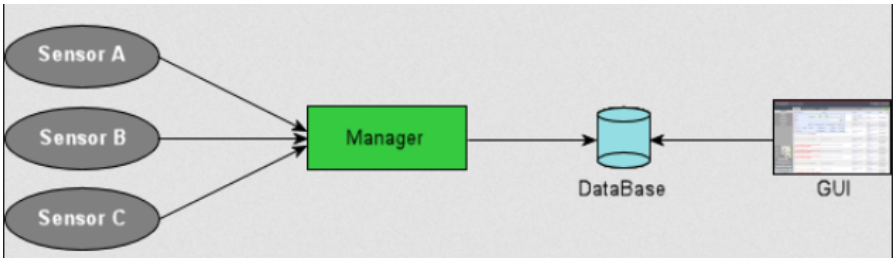

Abbildung 7: Einfache Architektur von Prelude
Quelle: (Prelude Team, 2007)

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

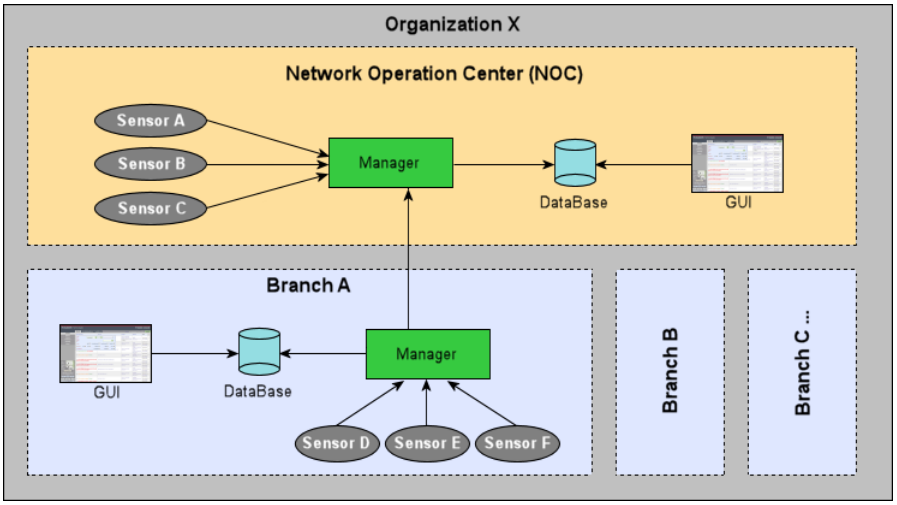

Abbildung 8: Erweiterte Architektur von Prelude mit der Nutzung von dezentralisierten Datenquellen und Bearbeitung
Quelle: (Prelude Team, 2007)

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 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 technischen Kriterien lag Prelude auf dem dritten Platz und in den benutzerfreundlichen Kriterien bekam Prelude den ersten Platz.

Auch in den nicht wissenschaftlichen Publikationen existiert eine begrenzte Anzahl von Texten über Preludes. Die existierenden Texten kommentieren ganz zusammenfassend über 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 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 behauptet auch, dass sein Tool in der Lage ist, Schwachstelle und Angriffe zu erkennen, Verhältnis zu beobachten und Daten Zusammenhang 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 anderen Version stammen (AT&T Cybersecurity, 2022).

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

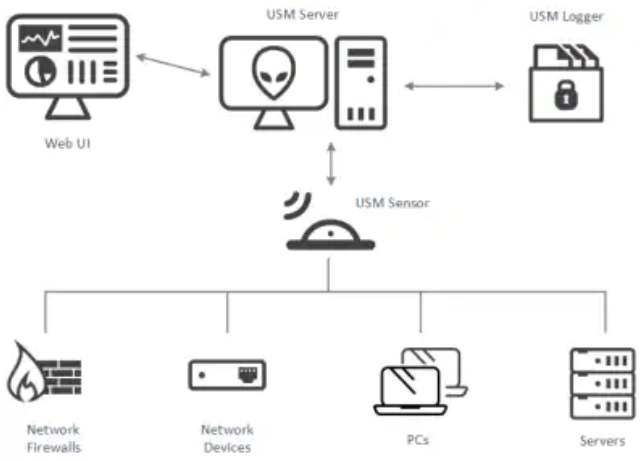

Abbildung 9: Architekturdiagramm ram von AlienVault USM
Quelle: (AT&T Cybersecurity, 2022)

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 Schwachstellen-Scanner 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 wegen ihre niedrigen Kosten besser für kleine oder mittelständige 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 Quelle eine manuelle Normalisierung der Logdatein 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 das kostenpflichtigen 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:

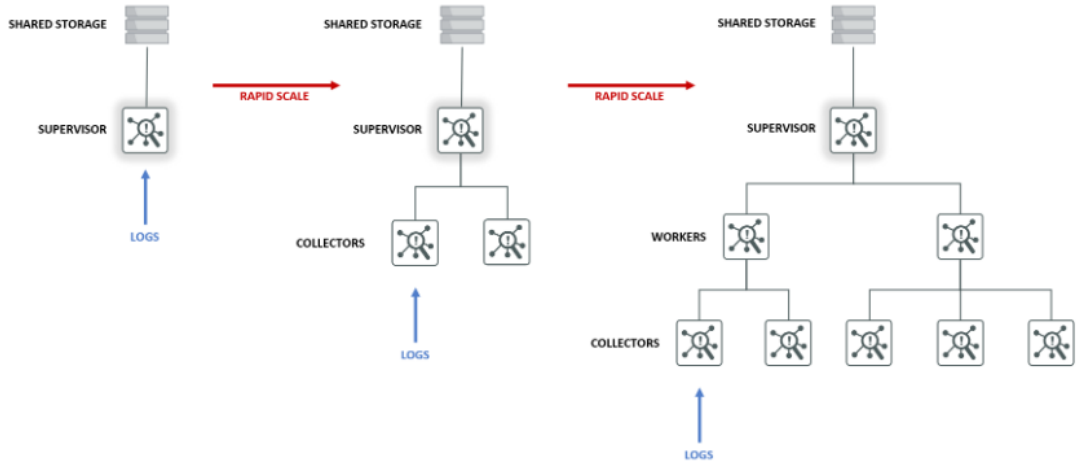

Abbildung 10: Skalierbare Architektur von FortiSIEM
Quelle: (Fortinet, 2020)

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 ürsprüngliche 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 von einer SIEM-Lösung und ist 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:

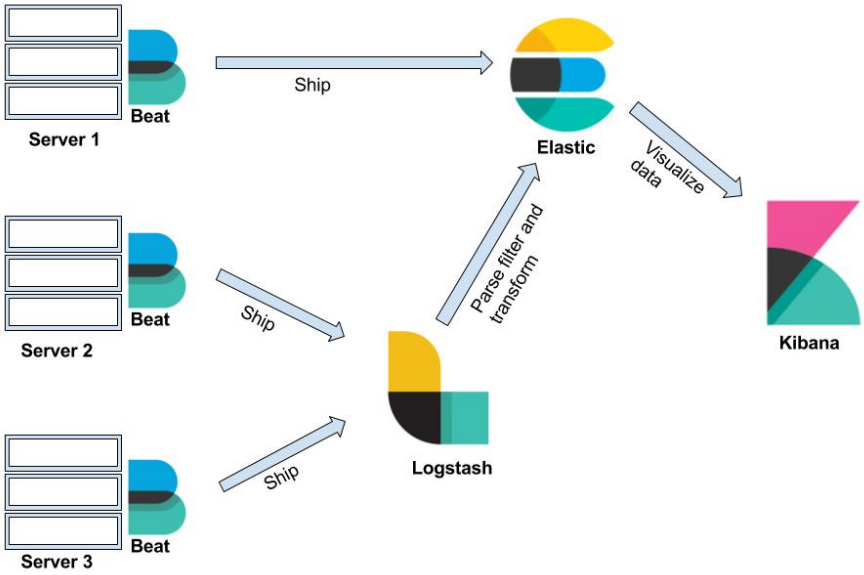

Abbildung 11: Integration zwischen Elasticsearch, Logstash und Kibana
Quelle: (packt, 2019)

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 wurde (Wang et al., 2019).

Die offiziele 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 por Element von ELK Stack:

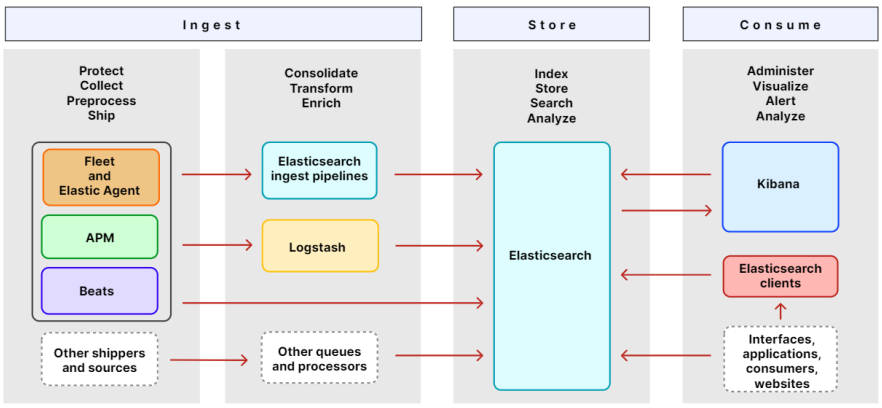

Abbildung 12: Aufteilung der Funktionalitäten zwischen den Komponenten
Quelle: (elastic, 2022)

Die wissenschaftliche Publikation über ELK Stack ist vielfältiger als bei der anderen recherchierten Tools. Es ist aber wichtig, zu betonen, dass die Mehrheit von denen sich eher mit dem Logging als mit den SIEM-Eingeschaften 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 Platform für Visualisierung von Data beschrieben. Mit dem Tool ist es möglich 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 ist auf Kibana3, 2.1.5, basiert. Ursprünglich sollte Grafana ein einfacheres Editingtool für Graphik sein und ermöglichen, Datenanfrage unkomplizierter zu machen. Die neuste

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

In der Webseite highlighted der Anbieter, dass Grafana die Zentralisierung und Zugang von Daten vereinfachen. Alle Art von Daten lassen sich analysieren und darstellen, von der Leistung von Anvwendungen 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 Loggin Tool Loki integriert, sodass Logdateien aus unterschiedlichen Quellen sich integrieren lassen. Auf dem Folgenden Bild wird die Struktur von Grafana für Logging dargestellt:

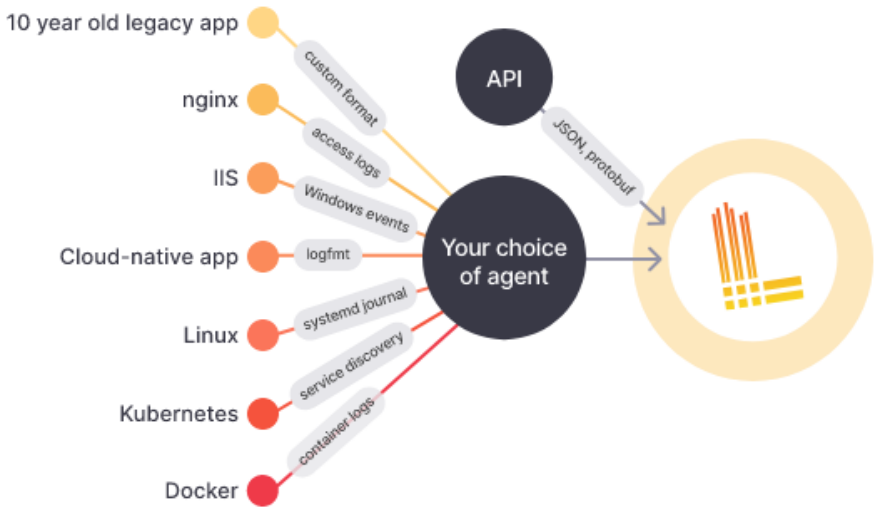

Abbildung 13: Integration von verschiedenen Log-Quellen mit Grafana Loki
Quelle: (Grafana Labs, 2022)

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 analyisiert werden. Die Warnmelund lässt sich auf 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).

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

2.2 Auswahlkrietieren

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 Source Tool, 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

3.1 Installation von SIEM in Container

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

- Implementation in Container

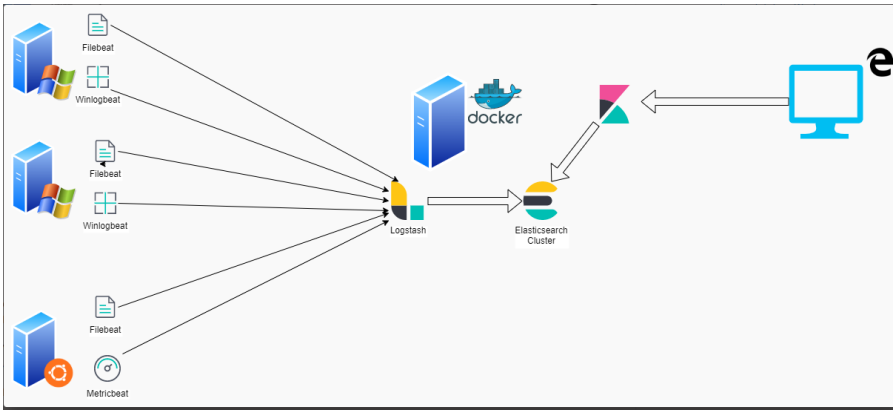

Abbildung 14: Struktur von SIEM in einem Container
Quelle: (RDR_IT, 2022)

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 07.03.2023.

AT&T Cybersecurity (2022). Alienvault ossim.
https://cybersecurity.att.com/products/ossim. Zugriff am 05.03.2023.

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. 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.

elastic (2022). *Elastic Docs*.
https://www.elastic.co/guide/en/welcome-to-elastic/current/new.html. Zugriff am 5.02.2023.

European Comission (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/2016/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_Collateral/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. 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.

Harmes, T. (2023). It-sicherheitsgesetz 2.0. https://rz10.de/knowhow/it-sicherheitsgesetz-2-0/. Zugriff am 04.03.2023.

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 (2018). Frequently Asked Questions.
https://attack.mitre.org/resources/faq/. Zugriff am 12.03.2023.

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/ch01lvl1sec10/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., 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 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%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.

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., Vlajic, 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. 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. 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.

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. 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.

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 Goczyła, 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.