



SIEM für Laborumgebungen

Security Information and Event Management für Laborumgebungen

Bachelorthesis FS24

Studiengang:	BSc Informatik
Autor:	Sven Trachsel
Betreuer:	Hansjürg Wenger
Experte:	Thomas Jäggi
Datum:	11.06.2024

Abstract

Die Menge an Systemen und damit Datenquellen in modernen IT-Infrastrukturen wächst ständig. Ohne automatisierte Abläufe können System- und Sicherheitsverantwortliche keinen Überblick über grosse Systemumgebungen behalten. Ein SIEM sammelt Logdaten, Alerts, Software-Bestände und Metadaten und stellt aus diesen Daten Alerts, Dashboards und aggregierte Datenquellen für weitere Analysen bereit. SIEM sind zentral für die IT-Security in Netzwerken und werden immer wichtiger, je grösser ein Netzwerk wird.

Das BFH-Cyberlab befindet sich aktuell im Aufbau und benötigt in Zukunft eine SIEM-Lösung, welche die Visibilität im Netzwerk gewährleistet. Passend zu den Anforderungen, welche im Verlauf der Arbeit erarbeitet wurden, hat die Evaluation eine taugliche Open-Source-Lösung ergeben. Mit «Wazuh» können Dashboards erstellt und bei Bedarf Alerts per E-Mail versendet werden. Ein Client sammelt nötige Daten von Endpunkten aller gängigen Betriebssysteme und sendet sich an das zentrale SIEM. Dort werden die Daten analysiert und für spätere Auswertungen und Dashboards archiviert. Wenn Regeln ein Security-Event feststellen, wird eine entsprechende Meldung versendet.

Das «Proof of Concept» zeigt eine Installation von Wazuh im Playground des BFH-Cyberlab. Unter Berücksichtigung der Anforderungen an Funktion und Sicherheit wurde Wazuh auf einem Server installiert. Diverse Maschinen im Playground wurden mit dem Wazuh-Agenten versehen und damit an das SIEM angebunden. Das System hat die gestellten Anforderungen erfüllt und kann in Zukunft im Cyberlab eingesetzt werden. Dazu wurde ein Konzept zur Überführung in den produktiven Betrieb erstellt.

Inhaltsverzeichnis

1	Einleitung	4
2	SIEM Allgemein	5
3	Marktübersicht	12
4	Requirements-Engineering	16
5	Proof of Concept	24
6	Schlussfolgerungen/Fazit	36
7	Abbildungsverzeichnis	38
8	Tabellenverzeichnis	39
9	Abkürzungsverzeichnis	40
10	Glossar	41
11	Literaturverzeichnis	42
12	Anhang	44
13	Selbständigkeitserklärung	76

1 Einleitung

In dieser Bachelor-Arbeit soll eine «Security Information and Event Management»-Lösung (kurz SIEM) für Laborumgebungen evaluiert und als Proof of Concept implementiert werden. Die Arbeit gliedert sich in einen theoretischen Teil, welcher Informationsbeschaffung zum Thema enthält, sowie einen praktischen Teil, welcher sich mit dem Finden und Implementieren einer geeigneten Lösung beschäftigt.

1.1 Aufgabenstellung

Auszug aus Aufgabenstellung auf Moodle «P24-Trachsel.pdf» (Hj. Wenger, 2024)

Ausgangslage:

In den Network and Security und den Cyber-Security Lab Umgebungen der BFH TI Informatik soll die Sichtbarkeit von sicherheitsrelevanten Ereignissen (Events) und Vorfällen (Incidents) verbessert werden.

Ein Security Information and Event Management (SIEM) kombiniert die zwei Konzepte Security Information Management (SIM) und Security Event Management (SEM) für die Echtzeitanalyse von Sicherheitsalarmen aus den Quellen: Anwendungen und Netzwerkkomponenten.

Zielsetzung:

Im Rahmen der Bachelorarbeit soll eine SIEM-Lösung für die bestehenden Laborumgebungen evaluiert und implementiert werden. Dabei sollen möglichst bestehende Datenquellen wie System-Logs, Flow-Daten, Netzwerk-Sensoren usw. gesammelt, zentral gespeichert und ausgewertet werden.

Beim Erkennen von Vorfällen (Incidents) soll eine Benachrichtigung erfolgen und gegebenenfalls automatisch Gegenmassnahmen eingeleitet werden.

Die gesammelten Daten können später auch für forensische Analysen verwendet werden.

Vorgehen:

- Marktübersicht über existierende SIEM-Lösungen erstellen
- Evaluation einer für die geplante Anwendung geeigneten Lösung
- Implementieren und Austesten dieser Lösung in einer Laborumgebung

1.2 Zieldefinitionen

Diese in der zweiten Projektsitzung definierten Ziele sind in Muss- und Kann-Ziele unterteilt. Während der Arbeit sollen die Ziele, mit einem Fokus auf Muss-Ziele, erreicht werden.

ZIEL-NR.	ZIELBESCHREIBUNG
M1	Der Bericht enthält eine Einführung in «SIEM»
M2	Der Bericht enthält eine Marktübersicht über SIEM-Lösungen
M3	Die Anforderungen an die SIEM-Lösung für Laborumgebungen wurden aufgenommen
M4	Eine Evaluation der SIEM-Lösung für Laborumgebungen wurde durchgeführt
M5	Ein Proof of Concept der evaluierten Lösung wurde erstellt
M6	Die Anforderungen aus Ziel «M3» wurden mit dem PoC aus Ziel «M5» abgeglichen
M7	Der Bericht enthält einen Vorschlag zur Überführung des PoC aus Ziel «M6» in den produktiven Betrieb

Tabelle 1 Zieldefinition "Muss"

ZIEL-NR.	ZIELBESCHREIBUNG
K1	Der Bericht enthält eine Erklärung des IDMEF (Intrusion Detection Message Exchange Format)
K2	Die Marktübersicht aus Ziel «M2» enthält eine Übersicht von Produkten, welche sich als SIEM-Bezeichnen, aber nicht unter die Definition fallen
K3	Die PoC-Lösung aus Ziel «M6» wurde in eine produktionsreife Lösung umgebaut

Tabelle 2 Zieldefinition "Kann"

2 SIEM Allgemein

SIEM steht für «Security Information and Event Management» und kombiniert Funktionen aus SIM (Security Information Management) und SEM (Security Event Management). Um den Begriff des SIEM genauer zu erläutern, müssen also zuerst die Begriffe SIM und SEM geklärt werden.

Die Aufgabe eines SIM-Systems besteht darin, Log-Daten zu sammeln und bereitzustellen. SIM-Systeme werden auch als Log Management bezeichnet.

Diese Systeme bieten auch die Möglichkeit, Analysen und Auswertungen über Logs zu erstellen und zu einfachen Events Alarmmeldungen zu versenden.

Zur Erkennung und Alarmierung bei komplexeren Abläufen über mehrere Log-Quellen hinweg wird ein SEM benötigt. Ähnlich wie ein IDS/IPS System löst es Alarme anhand vordefinierter Regeln auf, wenn verschiedene Security Events auftreten.

Die Kombination der beiden Konzepte SIM und SEM ist als Weiterentwicklung der Systeme zu verstehen. Ein SIEM kann alles, was ein SIM und SEM auch können und kombiniert die Verwaltung dieser Systeme in einem.

Auch vor diesem Bereich macht Machine-Learning keinen Halt, so sind sogenannte SIEM 3.0-Systeme oft mit Machine-Learning Mechanismen ausgestattet, welche Bedrohungen möglichst früh in der Cyber-Killchain erkennen sollen.

Datenquellen SIEM-Systeme sind jegliche Systeme, welche Sicherheitsrelevante Meldungen generieren können.

Offensichtliche Datenquellen sind hierbei Sicherheitssysteme wie Endpoint-Security in Form von Antivirus, EDR (Endpoint Detection and Response) oder XDR (Extended Detection and Response).

Diese generieren durch ihre Arbeit hauptsächlich Sicherheitsrelevante Meldungen. Auch Firewalls und IDS/IPS (Intrusion Detection / Intrusion Prevention System) Systeme gehören in diese Kategorie und generieren durch ihre Funktion hauptsächlich Sicherheitsrelevante Meldungen.

Server und Client-Betriebssysteme haben selbst auch Logs, welche für ein SIM und SIEM relevant sind. Auf Netzwerkebene lassen sich durch Netflows ebenfalls wertvolle Einblicke gewinnen, diese werden von Switches und Routern exportiert.

Folgende Systeme eignen sich insbesondere als Datenquelle für SIEM:

- Betriebssystem-Logs
 - Windows Event Log
 - Linux syslog / journald
- Client-Security-Software
 - Endpoint Detection and Response (EDR)
 - Extended Detection and Response (XDR)
 - Antivirus-Software
- Applikations-Logs
 - Webserver Access- und Error-Logs
 - SQL-Logs
 - ...
- Netflows
 - Switches
 - Router
 - Intrusion Detection/Prevention System (IDS/IPS)
- Logs von Netzwerksicherheits-Equipment
 - Firewalls
 - IDS/IPS
- Eigene Client-Software / Agenten

Folgende Grafik zeigt einige Datenquellen und wie diese mit dem SIEM interagieren. Alerts und Zugriffe auf das Dashboard sind auch visualisiert.

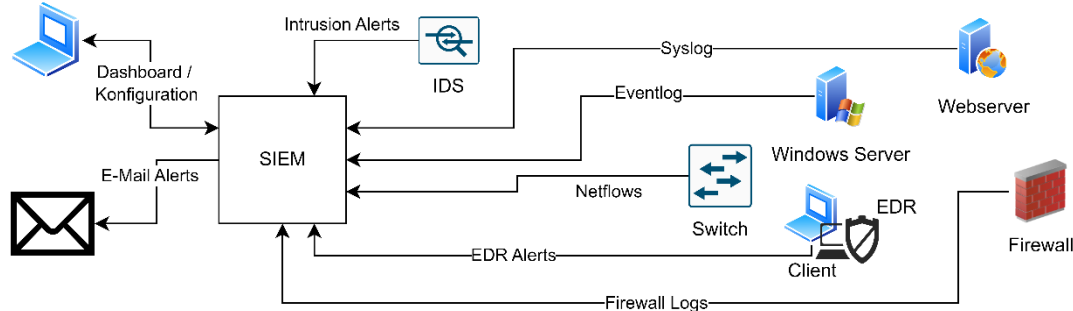


Abbildung 1 Diagramm SIEM Datenquellen

Ein Security Event ist eine Abweichung des Verhaltens eines Systems vom normalen Verhalten. Der Auslöser hierfür ist eine Bedrohung oder eine Sicherheitslücke. Nicht jedes Security Event wird zum Security Incident und damit zum Problem. Die Klassierung als Incident wie sie im folgenden Diagramm ersichtlich ist, ist Aufgabe des SEM.

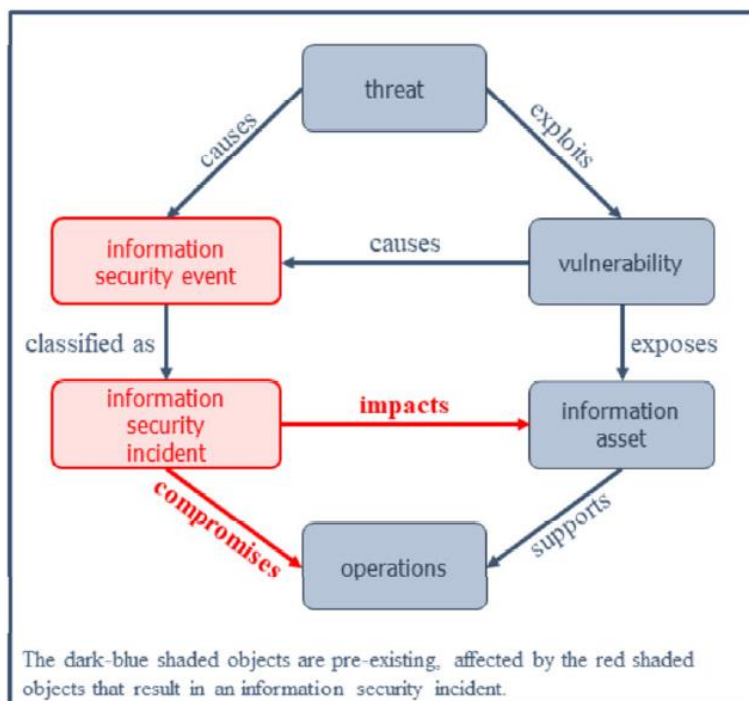


Abbildung 2 Zusammenhang Event und Incident

Quelle: Unterlagen BTI4204, S24.01 - Information Security.pdf, wgh1

Da sich diese Systeme so sehr ähneln, werden die Begrifflichkeiten auch von den Herstellern nicht immer im selben Kontext verwendet. Dies erschwert allfällige Recherche zu diesem Thema. Einige Produkte, welche sich gemäss der oben aufgeführten Definition nicht als SIEM klassifizieren, werden trotzdem als solche beworben.

Neben dem Erkennen von Bedrohungen eignen sich SIEM-Systeme auch als Grundlage für Datenanalysen und Fehlerbehebung, da sie die Logs aller Systeme im Netzwerk zentral sammeln. Die Kontrolle von vorgegebenen System-Verfügbarkeiten und Compliance-Anforderungen sind Dinge, welche sich mit einem SIEM gut bewerkstelligen lassen.

2.1 Aufbau eines SIEM

Ein SIEM sammelt Daten aus den in Kapitel 2 definierten Quellen. Dies wird bei Systemen, wo sich Client-Software installieren lässt durch einen Logcollector erreicht, welcher die Logdaten findet, in ein gemeinsames Format bringt, sie möglicherweise mit weiteren Informationen wie Geo-Information zu IP-Adressen anreichert und anschliessend in der SIEM-Datenbank ablegt.

Bei Systemen, welche keine Installation von Software zulassen, wie das z.B. bei Netzwerk-Hardware der Fall ist, können Logmeldungen auch via SIEM-Forwarder empfangen und in der SIEM-Datenbank abgelegt werden. Folgendes Diagramm veranschaulicht diesen Ablauf.

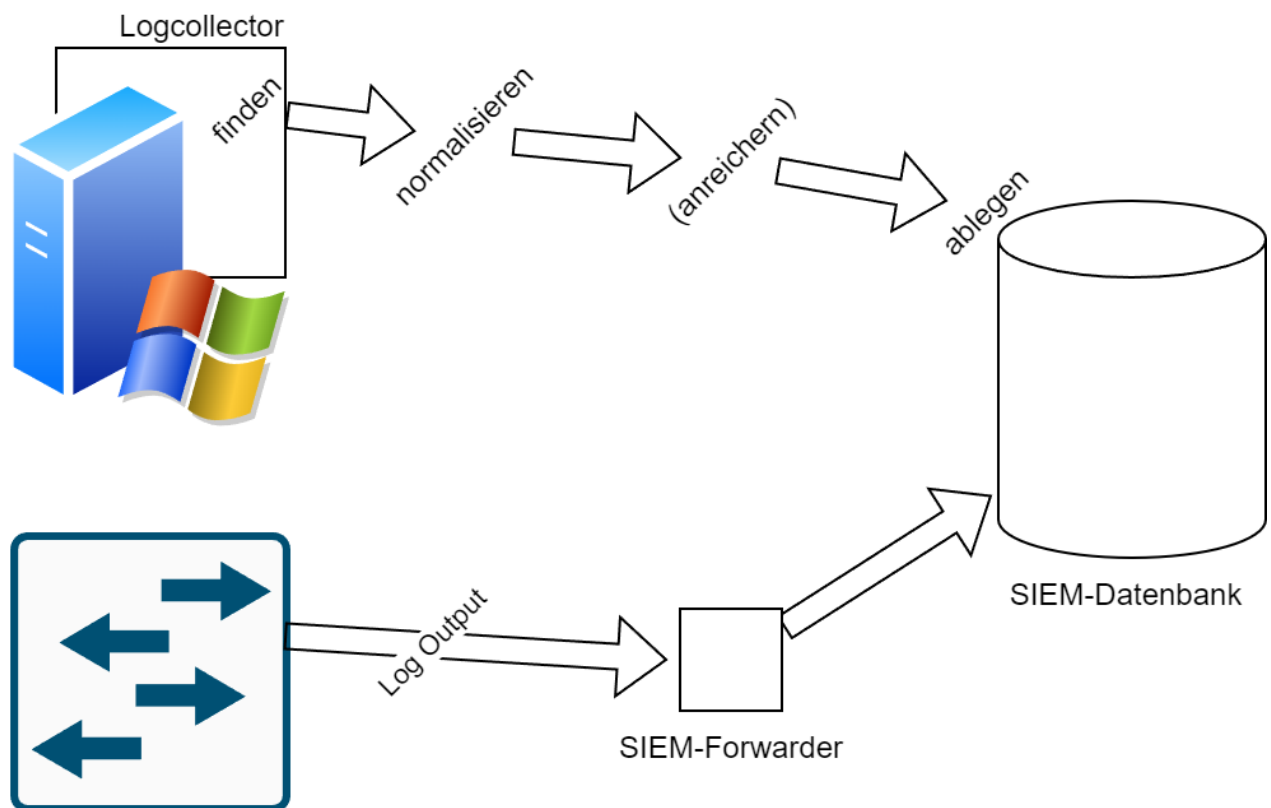


Abbildung 3 Diagramm SIEM Aufbau

Die abgelegten Daten werden vom SIEM anhand von SIEM Use-Cases analysiert. Dies sind Regeln, welche definieren in welchem Fall ein Event als Security-Incident eingestuft wird.

Anhand dieser Incidents können dann weitere Aktionen wie z.B. die Benachrichtigung eines Administrators erfolgen.

Der Ablauf nach dem Alarm muss durch Security Incident Management definiert werden. Nur so kann gewährleistet werden, dass bei einem Alarm das Richtige geschieht.

Folgendes Bild zeigt den High-Level-Aufbau eines SIEM.

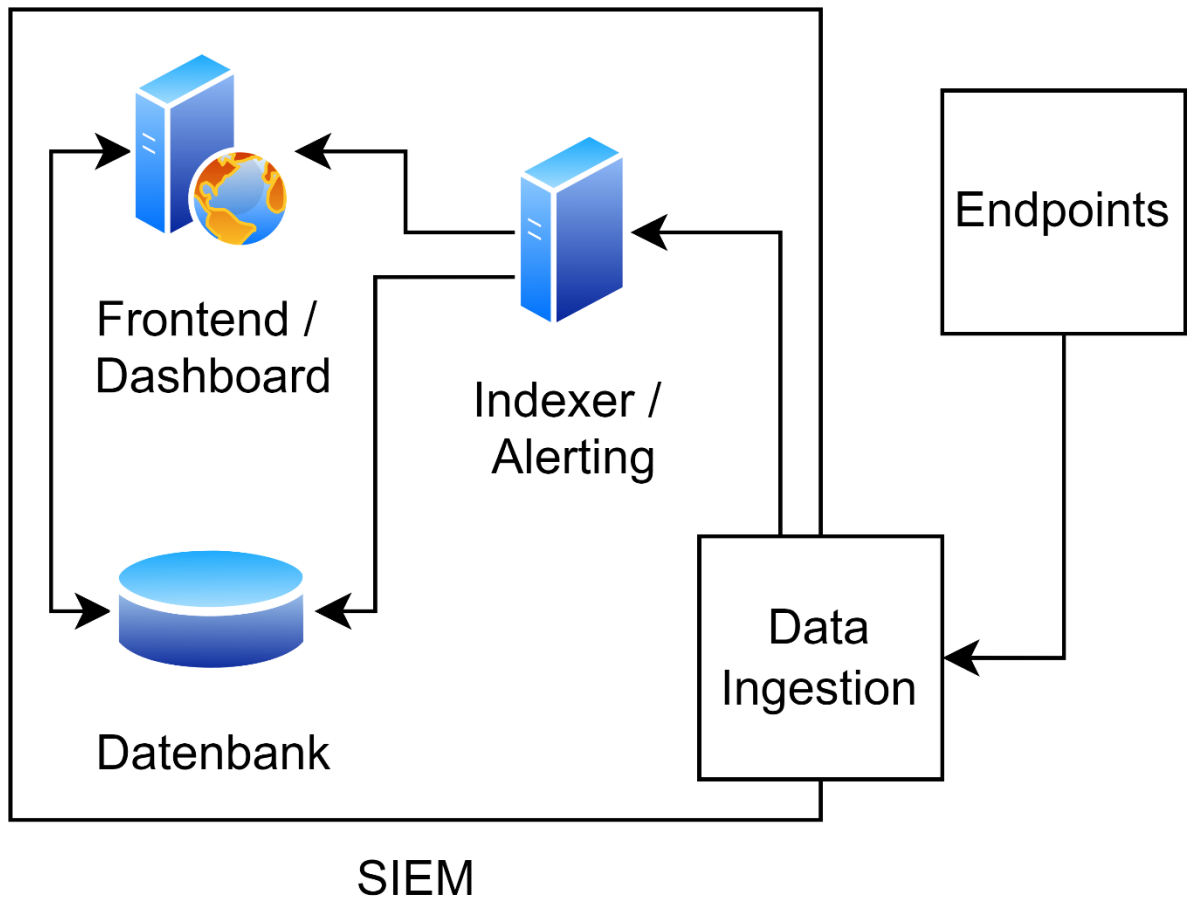


Abbildung 4 Diagramm SIEM Aufbau intern

Sind die Daten im SIEM angekommen werden sie auf verschiedene Arten verarbeitet. Der Indexer legt Daten wo nötig zu Archivzwecken ab, dies ermöglicht später einen Zugriff vom Dashboard aus oder Analysen vergangener Ereignisse. Falls die Daten eine erstellte Regel auslösen, so wird ein Alarm versendet, dass die Bedingungen für ein Security-Event eingetroffen sind. Das Dashboard ermöglicht Zugriff auf die erhaltenen Daten und erlaubt die Konfiguration des SIEM.

2.2 Definition SIEM

Was ist nun genau ein SIEM? Und was nicht?

Ein SIEM ist ein System, welches die Eigenschaften eines SIM und die Eigenschaften eines SEM in einem System vereint.

Folgende Grafik zeigt dies auf.

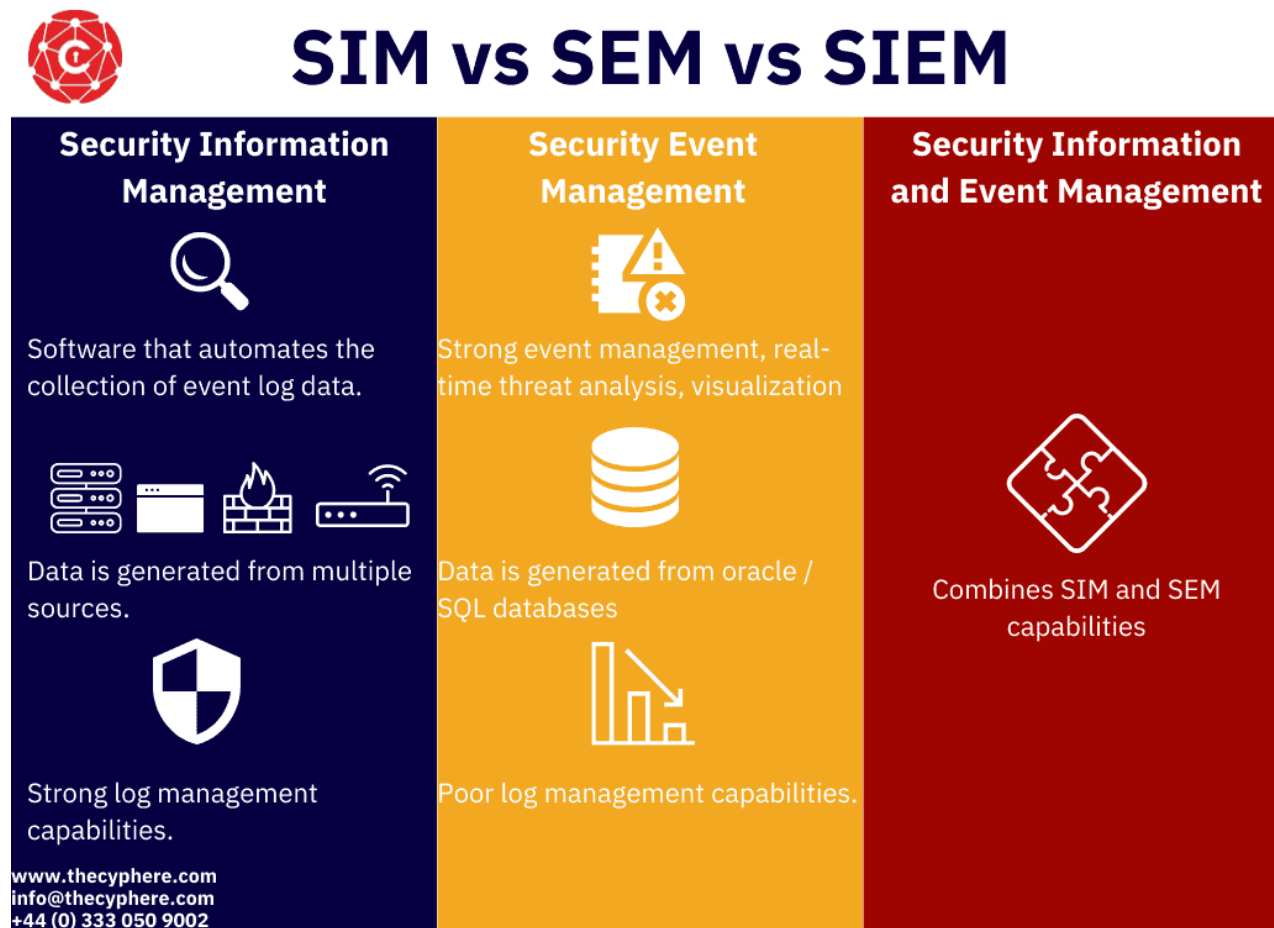


Abbildung 5 Grafik SIM vs. SEM vs. SIEM

Quelle: <https://thecyphere.com/blog/what-is-siem/>

Das System muss also Daten von verschiedenen Quellen sammeln können, gute Log-Management Eigenschaften haben, diese Daten in einer Datenbank für weitere Analysen speichern und Analysen auf diesen Daten machen, um Gefahren zu erkennen.

Diese Datensammlung wird an einem zentralen Ort angelegt.

Nur wenn ein System all diese Eigenschaften erfüllt, ist es eindeutig als SIEM zu bezeichnen.

2.3 Intrusion Detection Message Exchange Format

Gemäss RFC 4765, Quelle: <https://www.ietf.org/rfc/rfc4765.txt>

Um den Datenaustausch zwischen IDS, IPS, HIDS und auch SIEM-Systemen zu vereinheitlichen wurde im Jahr 2007 das «Intrusion Detection Message Exchange Format», kurz IDMEF, als experimentelles RFC eingereicht.

Es handelt sich um ein Nachrichtenformat, welches Daten in XML-Klassen kapselt und so strukturiert versendbar macht.

Folgende Grafik illustriert den Aufbau und die Varianten einer IDMEF-Message.

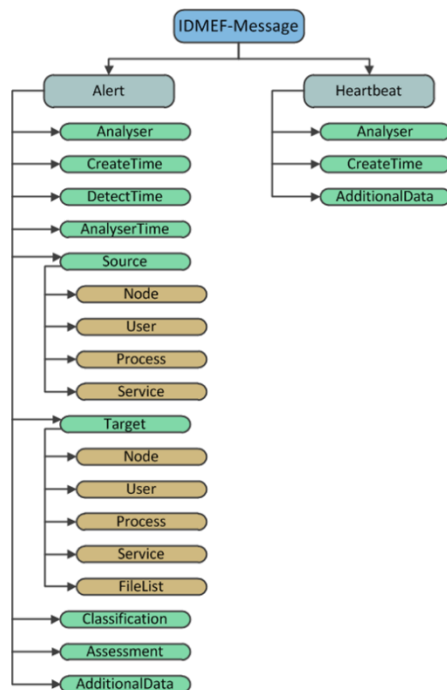


Abbildung 6 IDMEF Schema

Quelle: <https://upload.wikimedia.org/wikipedia/commons/9/9a/IDMEF-Schema.png>

Eine IDMEF-Message wird für Heartbeats und zum Versenden von Alerts verwendet.

Die Idee von IDMEF ist, dass Analyzer-Software auf einem Endpunkt, Daten über Alerts an einen Manager (z.B. SIEM) schickt.

Heartbeat

Heartbeat-Messages haben den Nutzen, dass der Manager sich über den Zustand eines Analyzers sicher sein kann. Ein Analyzer kann in einem vorgegebenen Intervall Heartbeat-Messages an den Manager senden, welcher der Manager auswerten kann, und bei Ausbleiben von Heartbeats Informationen über das Ausfallen eines Analyzers bekommt.

Ein Heartbeat hat folgende Inhalte:

Klasse	Beschreibung
Analyzer	Die Identifikation des Endpunktes, welche den Heartbeat generiert hat.
CreateTime	Der Zeitstempel, wann der Heartbeat erstellt wurde.
HeartbeatInterval	Das Intervall zwischen Heartbeats.
AnalyzerTime	Die aktuelle Zeit auf dem Analyzer bzw. Endpunkt.
AdditionalData	weitere Informationen

Tabelle 3 IDMEF Heartbeat Inhalt

Alert

Event-Messages werden für die Übertragung von Informationen über Incidents verwendet. Es gibt verschiedene Unterklassen von Alerts für spezifischere Incident-Meldungen, die Standard-Klasse

Ein Standard-Alert hat folgende Inhalte:

Klasse	Beschreibung
Analyzer	Die Identifikation des Endpunktes, welche den Alert generiert hat.
CreateTime	Der Zeitstempel, wann der Alert erstellt wurde.
Classification	Der Name des Alerts, damit das Problem klassifiziert werden kann.
DetectTime	Der Zeitstempel, wann das Event aufgetreten ist, welche zum Alert geführt hat.
AnalyzerTime	Die aktuelle Zeit auf dem Analyzer bzw. Endpunkt.
Source	Die Quellen des Events, welches zum Alert geführt hat.
Target	Die Ziele des Events, welches zum Alert geführt hat.
Assessment	Die Auswirkung des Alerts und Gegenmassnahmen, welche vom Analyzer vorgenommen wurden.
AdditionalData	Zusätzliche Informationen zu Event und Alert.

Tabelle 4 IDMEF Alert Inhalt

Einsatz und Relevanz

Das IDMEF wird von verschiedenen SIEM und HIDS-Systemen verwendet. Einige Open Source Beispiele sind Snort und Suricata als IDS/IPS, Sagan, OSSEC und Wazuh bei den SIEM.

Die SIEM-Systeme haben die Fähigkeit, solche Meldungen zu verarbeiten, sind jedoch nicht darauf angewiesen. Sie nehmen die Rolle eines Managers ein.

Im Jahr 2023 wurde ein Draft an das IETF gesendet, welches das IDMEF ersetzen soll. Das neue Format heisst IDMEFv2 und erweitert die Funktionen von IDMEF. Ausserdem standardisiert das Format auch den Austausch von Informationen zu physischem Eindringen, nicht nur die Cybersecurity.

3 Marktübersicht

Auf dem SIEM-Markt gibt es viele Angebote, welche sich teilweise sehr ähneln. Manche Hersteller bieten gleich mehrere Produkte in dieser Kategorie an und von Open-Source-Systemen gibt es Forks, welche dann als eigene System weiterexistieren.

Die bekannte IT-Research-Plattform «Gartner» listet im März 2024 81 verschiedene Produkte im Bereich «Security Information and Event Management».

Um hier einen Überblick zu erhalten, beschränkt sich diese Marktübersicht auf Systeme, welche vom Online-Magazin «Geekflare» in den Artikeln zu SIEM und Open-Source-SIEM gelistet wurden.

3.1 Methodik

Die Übersicht enthält Systemen, welche in den Artikeln von «Geekflare», welche im Literaturverzeichnis vermerkt sind, behandelt werden.

Artikel «Open Source SIEM Systems»

- AlienVault OSSIM
- Wazuh
- Sagan
- Prelude OSS
- OSSEC
- Snort
- Elastic Stack

Artikel «SIEM-Tools»

- Fusion SIEM
- Graylog
- IBM QRadar
- LogRhythm
- SolarWinds
- Splunk
- Elastic Security
- InsightIDR
- Cloud SIEM Enterprise
- NetWitness
- AlienVault OSSIM

Doppelte Einträge werden nur einmal aufgeführt.

Zusätzlich werden die hier folgenden Systeme aus persönlichem Interesse in die Übersicht aufgenommen.

Alle behandelten Systeme sind im Gartner-Verzeichnis zu SIEM enthalten.

Persönliches Interesse

- FortiSIEM
- Microsoft Sentinel

Folgende Attribute sollen für die untersuchten Systeme aufgeführt werden. Die Tabelle beschreibt, wie die Attribute heissen und wie sie sich auszeichnen.

Attribut-Name	Beschreibung
Name	Die Bezeichnung des Systems durch den Hersteller.
Hersteller	Der Hersteller der Software.
Lizenz	Die Lizenz, unter welcher die Software angeboten wird.
Gartner-Bewertung	Die Bewertung gemäss Verzeichnis von Gartner Stand März 2024. Bestehend aus der Bewertung zwischen 1 und 5, sowie der Anzahl abgegebener Bewertungen
Bemerkung	Welche Funktionen zeichnen diese SIEM-Lösung aus, in Stichworten.

Tabelle 5 Beschreibung Bewertungskriterien

Die Tabellenvorlage gemäss den oben genannten Punkten sieht folgendermassen aus.

Name	Hersteller	Lizenz	Gartner-Bewertung	Funktionen
System 1				
System 2				

Tabelle 6 Vorlage Marktübersicht

Mit dieser Vorlage wird die Marktübersicht des folgenden Kapitels ausgearbeitet.

3.2 Ausarbeitung Marktübersicht SIEM

Die zusammengetragenen Daten sind in der nachfolgenden Tabelle aufgeführt. So ist eine einfache Unterscheidung der Systeme anhand der Kriterien Hersteller, Lizenzierung, Beliebtheit und Funktionsumfang möglich. Dieses Wissen wird als Grundlage für das darauffolgende Requirements-Engineering verwendet.

Name	Hersteller	Lizenz	Gartner-Bewertung	Bemerkung
AlienVault OSSIM	AT&T	GNU GPL v2	4.4 (75) ¹	SIEM-Features ohne Log Management
Cloud SIEM Enterprise	Sumo Logic	proprietär	4.6 (112)	SIEM ausschliesslich als SaaS
Elastic Stack / Security	Elastic NV	Elastic License 2.0 ²	4.4 (364)	aufbauend auf Elastic Stack,
FortiSIEM	Fortinet	proprietär	4.6 (146)	SIEM als Teil des Fortinet-Ökosystems
Fusion SIEM	Exabeam	proprietär	4.6 (243)	Cloud Lösung, inklusive XDR
Graylog Open	Graylog	SSPL ³	4.3 (162)	Cloud-Anbindung (Produkte) kostenpflichtig
IBM QRadar	IBM	proprietär	4.3 (564)	als SaaS und On-Premise verfügbar
InsightIDR	Rapid7	proprietär	4.3 (310)	nur in der Cloud
LogRhythm SIEM	LogRhythm	proprietär	4.5 (693)	Inklusive XDR, Fokus auf Automation
Microsoft Sentinel	Microsoft	proprietär	4.4 (71)	Passt in Microsoft Ökosystem, nur in Azure Cloud
NetWitness	NetWitness	proprietär	4.4 (117)	Fokus auf Skalierbarkeit
OSSEC	OSSEC Project	GNU GPL v2	nicht gelistet	Mehr Features mit Registrierung (gratis), bezahlte Vollversion, als HIDS gelistet, ELK-Integration
Prelude OSS	Prelude	GNU GPL v2	nicht gelistet	Keine Aktivität ersichtlich (ev. nicht mehr weiterentwickelt)
Sagan	Quadrantsec	GNU GPL v2	nicht gelistet	letzter Release im Dezember 2021
Snort	Cisco	GNU GPL v2 ⁴	nicht gelistet	Netzwerk IDS, kein vollständiges SIEM
SolarWinds SEM	SolarWinds	proprietär	4.1	On-Premise, als SEM vermarktet
Splunk	Splunk	proprietär	4.4 (832) / 4.5 (451) ⁵	Cloud-basiert, Marktführer gemäss Gartner
Wazuh	Wazuh Community	GNU GPL v2	4.7 (10)	Fork von OSSEC, implementiert wie OSSEC ELK Stack Neben SIEM auch XDR-Funktionen

Tabelle 7 Marktübersicht SIEM

¹ Bewertung von AlienVault USM (kostenpflichtige Vollversion)

² nicht als Open-Source anerkannt, bietet Gratis-Version mit weniger Features

³ Server Side Public License, nicht als Open Source anerkannt, von GNU GPLv3 abgeleitet, bietet Gratis-Version mit weniger Features

⁴ nur Source-Code, IDS-Regeln sind kostenpflichtig

⁵ 4.4 für Splunk Enterprise, 4.5 für Splunk Enterprise Security, was Splunk noch mit weiteren GUI-basierten Tools erweitert

3.3 SIEM-Kategorisierung

Dieses Kapitel beschäftigt sich mit Systemen, welche von einigen Quellen als SIEM bezeichnet werden, aber durch andere Quellen oder die Namensgebung Zweifel lassen, ob es sich dabei um ein SIEM handelt. Gemäss der Definition aus Kapitel 2.2 werden diese Systeme auf ihre Kategorisierung als SIEM untersucht.

Es werden Systeme behandelt, welche während der Ausarbeitung von Kapitel 3.2 aufgefallen sind.

3.3.1 AlienVault OSSIM

Durch die Namensgebung von AlienVault OSSIM lässt sich vermuten, dass es sich hauptsächlich um ein SIM handelt, welches die SEM-Eigenschaften nicht erfüllt.

Im Vergleich der Open-Source-Variante «AlienVault OSSIM» mit dem kommerziellen Produkt «AlienVault USM Anywhere» stellt sich das Gegenteil heraus. Die Feature-Matrix beschreibt das Fehlen einer Log-Management-Funktion bei OSSIM. Dies ist eine zentrale Funktion eines SIM, aber keine Stärke eines SEM.

Daten werden zentral auf einem Server gespeichert, was für ein SIEM spricht.

Durch das Fehlen der Log-Management Funktion fehlt dem Produkt die SIM-Komponente, was es zusammen mit den Intrusion Detection Features zu einem SEM macht. Es handelt sich also um kein SIEM nach der Definition aus Kapitel 2.2.

3.3.2 Snort

Snort ist ein Netzwerk Intrusion Prevention System (IPS). Das bedeutet, es ist ein Intrusion Detection System (IDS), welches mit Zugriff auf Firewalls konfiguriert werden kann, um bei einem Incident automatisch Firewall-Regeln anzupassen und die Gefahr so abzuwehren.

Das System ist auf Netzwerkverkehr ausgelegt, kann also nicht wie von einem SIEM gefordert, verschiedene Datenquellen anzapfen. Die Website beschreibt Snort als «Paket-Logger», was sich auch nur auf Netzwerkverkehr bezieht. Snort ist also auch kein Log-Management-System, wie es von einem SIEM gefordert ist.

Nach diesen Kriterien ist Snort ein SEM für einen einzelnen Host, es fehlen jedoch die SIM-Eigenschaften, um es zu einem SIEM zu machen. Auch die Zentralisierung ist hier nicht gegeben.

3.3.3 SolarWinds SEM

Der Name des Produkts lässt darauf schliessen, dass es sich dabei um ein SEM handelt, welchem die SIM-Eigenschaften fehlen, um unter die Definition eines SIEM zu fallen.

Neben den SEM-Features wie Threat-Management über Regeln und eine zentrale Datenspeicherung, bietet das System aber auch gutes Log Management, sowie Monitoring und Datensammlung von diversen Endpunkten.

Da dieses System sowohl die im Namen enthaltenen SEM-Funktionen als auch in der Definition enthaltene SIM-Funktionen bietet, ist es gemäss Kapitel 2.2 als SIEM zu klassifizieren.

Hier verspricht der Name weniger, als das System bieten kann. Das weiterführende Marketingmaterial spricht jedoch auch von SIEM-Funktionen, was korrekt ist.

4 Requirements-Engineering

Dieses Kapitel beschreibt im ersten Teil die Umgebung, in welcher ein SIEM bereitgestellt werden soll. Anforderungen an das SIEM werden aufgeführt. Danach wird eine Evaluation einer Lösung anhand der Anforderungen erstellt.

4.1 Stakeholder

Hier werden die verschiedenen Stakeholder und deren Erwartungen an das System beschrieben.

4.1.1 Beschreibung Stakeholder

Stakeholder werden hier aufgeführt und in einigen Sätzen beschrieben.

Laborteam

Das Team des BFH-Cyberlab besteht aus Security-Spezialisten. Diese Personengruppe möchte relevante Ereignisse erkennen und darauf reagieren können. Die Erkennung dieser Ereignisse dient einerseits der Sicherheit der Laborumgebung, aber auch der Forschung.

Insbesondere sollen im Labor stationierte Honeypots Ereignisse generieren, welche das Laborteam mit dem SIEM analysieren kann.

Dozierende

Die Gruppe der Dozierenden überschneidet sich mit dem Laborteam, ist aber nicht identisch.

Dozierende möchten ihren Studenten etwas zu IT-Security beibringen und bringen dazu möglicherweise Malware mit oder zeigen Angriffe auf Systeme im Labor vor. Werden diese Angriffe vom SIEM erkannt, so kann diese Meldung dem dozierenden bei der Lernveranstaltung eine gute Erweiterung des Materials sein.

Studenten

Studenten sind auch Benutzer des Labors und somit auch involviert, wenn das SIEM arbeitet. Das Interesse der Studenten besteht darin, über Bedrohungen zu lernen. Dies kann passieren, indem sie Angriffe von dozierenden selbst ausführen oder sich von dozierenden, Angriffe zeigen lassen. Auswertungen des SIEM können z.B. durch einen Bildschirm im Lehrraum angezeigt werden, was den Unterricht interaktiv gestaltet.

Management

Das SIEM soll «managementtaugliche» Darstellungen von Abläufen und Ereignissen bieten. Daten sollen übersichtlich dargestellt werden können, damit sich Vorgesetzte und andere Personengruppen schnell ein Bild der Geschehnisse machen können.

Besucher

Besucher sind Personen mit unbekanntem Informatik-Know-how, welche sich ein Bild des Labors machen möchten. Sie sind grundsätzlich interessiert, was passiert. Es muss davon ausgegangen werden, dass sie keinen Informatik-Hintergrund haben. Der Besucher möchte z.B. mittels grafischer Mittel ein Bild des Geschehens erhalten, dieses aber nicht vertieft verstehen.

Angreifer

Die Ziele eines externen Angreifers können unterschiedlich sein, meist jedoch sind diese schlussendlich monetärer Natur. Angreifer möchten unbemerkt Systeme infizieren und sich im Netzwerk festigen (Persistenz) um ihre übergeordneten Ziele zu erreichen. Dies erreichen sie, indem verschiedene Techniken und Schwachstellen zum Eindringen in Systeme verwendet werden.

4.1.2 Zielkonflikte

Die möglichen Zielkonflikte zwischen Stakeholdern sind hier beschrieben.

Angreifer gegenüber Laborteam

Die Ziele der Angreifer stehen im Konflikt zu den Zielen des Laborteams, welches eine persistente Infektion der Umgebung verhindern möchte. Den Zielen des Laborteams ist in diesem Fall vollumfänglich Priorität über deren der Angreifer zu geben, schliesslich ist es das Ziel des SIEM, Bedrohungen zu erkennen.

Management und Besucher gegenüber Laborteam

Die einfache Darstellung der Ereignisse allein reicht für die Bedürfnisse des Laborteams nicht aus. Erste Priorität haben SIEM-Funktionen, welche das Laborteam bei dessen Arbeit unterstützen. Diese schliessen ein weiteres Benutzerinterface mit vereinfachten Darstellungen und Übersichten jedoch nicht aus. Es ist möglich, die Ziele beider Parteien zu berücksichtigen. Sie stehen nicht direkt in Konflikt.

4.2 Systemumfeld

Hierbei handelt es sich um eine Beschreibung des Umfelds, worin das SIEM bereitgestellt werden soll.

Das SIEM soll im BFH-Cyberlab integriert werden. Dieses ist aktuell in der Entstehung. Die Beschreibung des Systemumfelds bezieht sich einerseits auf die aktuell bestehenden Infrastrukturen, zeigt aber auch zukünftige Pläne der Weiterentwicklung auf, wie sie während Besprechungen mit dem Lab-Team (siehe Sitzungsprotokolle in Anhang 12.2) aufgenommen wurden.

Das Cyberlab der BFH besteht aktuell aus 12 virtuellen Maschinen und 2 Hypervisoren. Switches, Firewalls und weitere physische Server sind auch vorhanden und weitere in Zukunft geplant. Es soll auch einmal möglich sein, das Labor um physische Maschinen zu erweitern.

Das Cyberlab unterteilt sich in zwei Bereiche, den Infrastrukturteil und den Playground-Teil. Auf der Seite der Infrastruktur befinden sich die Systeme, welche für die grundsätzliche Funktionalität des Labors benötigt werden. Diese Systeme sind als «produktiv» zu betrachten und dürfen nur mit den entsprechenden Vorsichtsmassnahmen und Sicherheit, dass die Systeme nach Änderungen immer noch laufen, modifiziert werden. Hier sind die Hypervisoren, und aktuell vorhandenen Switches und Firewalls angesiedelt.

Der Playground hat weniger Restriktionen und ist, dem Namen gerecht, als Spielplatz verwendbar. Hier können Maschinen schnell erstellt und auch von Studenten verwendet werden. Infektionen einzelner Maschinen sind nicht grundsätzlich problematisch. Es besteht ein Konzept, um die ganze Umgebung im Falle einer Infektion zu löschen und schnell wieder erstellen zu können. Das wird unter anderem mit Ansible-Scripts zur Automatisierung und Sicherstellung der Reproduzierbarkeit bewerkstelligt.

Im Playground befinden sich auch einige Honeypots in Form von Windows-Maschinen, welche der Malware-Analyse dienen.

Der Playground ist der Teil des Cyberlab, welcher für diese Bachelor-Thesis hauptsächlich relevant ist. Ein Proof of Concept wird im Playground erstellt, eine produktive Lösung soll später einmal im Infrastruktur-Teil des Cyberlab laufen.

4.3 Methodik Anforderungen an SIEM und Umsetzung

Hier werden die Anforderung an das SIEM für das Cyberlab, unterteilt in Anforderungen an das System selbst und Anforderungen an die Umsetzung, aufgeführt.

Das Verwendete Format entspricht einer Tabelle, wie folgt.

Nummer	Anforderung	Gewichtung
A1	Anforderung an SIEM 1	1
U1	Anforderung an Umsetzung 1	K.-o.

Tabelle 8 Vorlage Anforderungen

Nummer

Die Nummer bezeichnet die Anforderung eindeutig, «A» steht für eine Anforderung an das System, «U» für Anforderungen an die Umsetzung.

Anforderung

Dies ist die Bezeichnung der Anforderungen.

Gewichtung

Dies ist entweder eine Zahl zwischen 1 und 3, um die Gewichtung dieser Anforderung für die spätere Evaluation darzustellen, wobei 1 die niedrigste und 3 höchste Gewichtung ist, oder der Wert «K.-o.», welcher ein K.-o.-Kriterium bezeichnet, dessen nicht-Erfüllung das Ausscheiden der zu evaluierenden Lösung zur Folge hat.

4.3.1 Anforderungen an SIEM

Diese Anforderungen werden später zur Evaluation der SIEM-Lösung verwendet. Sie Beschreiben die Funktionen, welche eine Lösung haben soll. Es sind auch Anforderungen enthalten, welche die Art des Produkts beschreiben und nicht direkt eine Funktion.

Nummer	Anforderung	Gewichtung
A1	Open Source Lizenz	K.-o.
A2	Wird noch aktiv weiterentwickelt	K.-o.
A3	Erfüllt Kriterien eines SIEM	K.-o.
A4	Erkennung von Security Events	3
A5	Alarmierung bei Security Events	3
A6	Alarmierung nur bei Security Incidents (Unterscheidung zu Events)	2
A7	Daten für Dashboard bereitstellbar	2
A8	Lösung bietet ein ausführliches Dashboard	1
A9	Aktive Komponenten (Möglichkeit auf Incidents zu reagieren)	1

Tabelle 9 Anforderungen an das System

A1 Open Source Lizenz

Die Lösung muss unter einer Open-Source Lizenz vertrieben werden. Proprietäre Lösungen erfüllen dieses K.o.-Kriterium nicht, während von Open-Source abgeleitete Lizenzen einen Punkteabzug bekommen.

Nur in kostenpflichtigen Abo-Stufen verfügbare Funktionen werden in der Bewertung nicht berücksichtigt.

A2 Wird noch aktiv weiterentwickelt

Das System wird noch aktiv weiterentwickelt und «unterstützt». Überprüfbar durch Berichte, nach denen eine Lösung nicht mehr verwendet werden sollte und durch das Datum der letzten Code-Commits auf Github.

A3 Erfüllt Kriterien eines SIEM

Da ein SIEM evaluiert werden soll, muss die Lösung der SIEM-Definition gemäss Kapitel 2.2 entsprechen.

A4 Erkennung von Security Events

Das SIEM soll Security Events verschiedener Art erkennen können.

A5 Alarmierung bei Security Events

Das SIEM soll bei auftretenden Security Events einen Alarm auslösen können. Die Alarmierung soll per E-Mail erfolgen. Weitere Alarmierungsmöglichkeiten wie SNMP sind ebenfalls erwünscht. Eine Abgrenzung, bei welchen Events ein Alarm ausgelöst wird soll möglich sein.

A6 Alarmierung nur bei Security Incidents (Unterscheidung zu Events)

Das System soll zwischen Security Events und Incidents unterscheiden können und nur bei Incidents Alarme versenden können.

A7 Daten für Dashboard bereitstellbar

Gesammelte Daten sollen aus dem System für Dashboards zur Verfügung gestellt werden oder ein simples Dashboard ist verfügbar.

A8 Lösung bietet ein ausführliches Dashboard

Die Lösung bietet ausführliche Dashboards, um Daten zu visualisieren.

A9 Aktive Komponenten (Möglichkeit auf Incidents zu reagieren)

Die Lösung bietet aktive Gegenmassnahmen zu laufenden Angriffen. Diese Mechanismen werden oft als «XDR» bezeichnet.

4.3.2 Anforderungen an Umsetzung

Diese Anforderungen sind für die spätere Umsetzung eines Proof of Concept, sowie die Empfehlung für die Überführung in den produktiven Betrieb wichtig. Für die Evaluation werden sie nicht berücksichtigt, da sie beschreiben, wie mit der Lösung umgegangen werden soll.

Nummer	Anforderung	Gewichtung
U1	Konfigurationen sind nachvollziehbar	3
U2	Das System ist einfach reproduzierbar	3
U3	Security Considerations werden angestellt	2
U4	Die Konfigurationsphilosophie des BFH Cyberlab wird eingehalten	2

Tabelle 10 Anforderungen an die Umsetzung

U1 Konfigurationen sind nachvollziehbar

Die Konfiguration des Systems ist nachvollziehbar und dokumentiert.

U2 Das System ist einfach reproduzierbar

Das System lässt sich einfach reproduzieren, zum Beispiel durch Ansible-Scripts.

U3 Security Considerations werden angestellt

Die Umsetzung berücksichtigt Security Considerations des SIEM. Diese sind bei allfälligen XDR-Funktionen schwergewichtig zu behandeln, da dort Eingriffe an bestehenden Systemen vorgenommen werden.

U4 Die Konfigurationsphilosophie des BFH Cyberlab wird eingehalten

Die vom BFH Cyberlab-Team vorgegebene Konfigurationsphilosophie wird bei den nötigen Systemkonfigurationen eingehalten.

Diese beinhaltet «Secure Defaults», welche durch die Security Considerations abgedeckt werden und die Verwendung von Drop-In-Konfigurationen, wo möglich.

4.4 Evaluation

In der Evaluation werden die Systeme aus Kapitel 3 mit den Anforderungen aus Kapitel 4.3.1 verglichen und so eine passende Lösung für das Cyberlab der BFH ermittelt.

4.4.1 Filterung K.-o.-Kriterien

In einem ersten Schritt werden Systeme, welche die K.-o.-Kriterien nicht erfüllen, aussortiert.

A1 Open-Source Lizenz

Folgende Systeme haben kein Open-Source-Lizenzmodell und werden daher aussortiert.

- Cloud SIEM Enterprise
- FortiSIEM
- Fusion SIEM
- IBM QRadar
- InsightIDR
- LogRhythm SIEM
- Microsoft Sentinel
- NetWitness
- SolarWinds SEM
- Splunk

Die beiden Produkte «Elastic Stack / Security» und «Graylog Open» bieten zwar keine anerkannte Open-Source Lizenz, haben jedoch mit der «Elastic License 2.0» und «SSPL» Lizenzen, welche von Open-Source abgeleitet sind. Sie werden nicht aussortiert.

A2 Wird noch aktiv weiterentwickelt

Folgende Systeme werden nicht mehr aktiv weiterentwickelt und werden daher aussortiert.

- Prelude OSS
- Sagan

A3 Erfüllt Kriterien eines SIEM

Folgende Systeme erfüllen die Anforderungen an ein SIEM gemäss Kapitel 2.2 nicht und werden daher aussortiert. Die Begründung wurde in Kapitel 3.3 ausgeführt.

- AlienVault OSSIM
- Snort

4.4.2 Bewertung

Die folgenden Systeme sind nicht durch K.o.-Kriterien ausgeschieden und werden nun mit den Anforderungen aus Kapitel 4.3.1 bewertet.

- Elastic Stack / Security
- Graylog Open
- OSSEC
- Wazuh

Die K.o.-Anforderungen werden auch aufgenommen und mit 3 Punkten bewertet, da so noch eine genauere Aussage über den Erfüllungsgrad gemacht werden kann. Die Lösungen in der folgenden Tabelle haben die K.o.-Anforderungen grundsätzlich erfüllt.

Anforderung	Gewichtung	Elastic Stack / Security	Graylog Open	OSSEC	Wazuh
A1	3	1	1	3	3
A2	3	3	3	2	3
A3	3	3	3	3	3
A4	3	3	3	3	3
A5	3	2	3	3	3
A6	2	3	2	3	3
A7	2	3	3	3	3
A8	1	3	1	3	3
A9	1	1	1	3	3
Total		52	51	60	63

Tabelle 11 Bewertung Anforderungen SIEM

Folgend wird die Vergabe der Punktzahlen begründet.

A1 Open-Source Lizenz

Während OSSEC und Wazuh unter GNU GPLv2 vertrieben werden, sind die Lizenzen von Graylog Open und dem Elastic Stack nicht als Open Source anerkannt, jedoch davon abgeleitet.

A2 Wird noch aktiv weiterentwickelt

Während der Elastic Stack und Graylog Open Firmen hinter sich haben, sind OSSEC und Wazuh Community-Projekte. Wazuh ist ein Fork von OSSEC und obwohl OSSEC immer noch weiterentwickelt wird ist ein Teil der Community zu Wazuh übergegangen.

A3 Erfüllt Kriterien eines SIEM

Alle Produkte erfüllen die Definition eines SIEM gemäss Kapitel 2.2.

A4 Erkennung von Security Events

Alle Produkte können Security-Events erkennen.

A5 Alarmierung bei Security Events

Alle Produkte können Alerts per E-Mail versenden. Im Elastic-Stack können die Benachrichtigungen jedoch nur angepasst werden, wenn eine kostenpflichtige Version verwendet wird.

A6 Alarmierung nur bei Security Incidents (Unterscheidung zu Events)

Graylog Open bietet in der gratis-Version nur ein einfaches Alerting-System. Bessere Features wie sie bei den Open-Source Varianten und dem Elastic Stack vorhanden sind, sind kostenpflichtig.

A7 Daten für Dashboard bereitstellbar

Alle Lösungen bieten ein simples Dashboard.

A8 Lösung bietet ein ausführliches Dashboard

Die ausführlichen Dashboards sind bei Graylog Open kostenpflichtig. Elastic, OSSEC und Wazuh bieten Übersichtliche Dashboards von Haus aus an.

A9 Aktive Komponenten (Möglichkeit auf Incidents zu reagieren)

Bei Elastic und Graylog sind XDR-Funktionen kostenpflichtig, OSSEC und Wazuh bieten diese Funktionen an.

4.5 Variantenentscheid

Die Bewertung in Kapitel 4.4.2 in der Tabelle 11 hat folgende Resultate erbracht:

System	Punktzahl
Elastic Stack / Security	52
Graylog Open	51
OSSEC	60
Wazuh	63

Tabelle 12 Resultate SIEM Bewertung

Die maximale Punktzahl liegt bei 63 Punkten.

Diese wurde von Wazuh erreicht, die anderen Lösungen haben weniger Punkte erreicht.

Für das BFH-Cyberlab ist die evaluierte Lösung somit «Wazuh».

4.6 Gefundene Lösung im Detail

Gemäss Wazuh Webseite, Quelle: <https://wazuh.com/platform/overview/>

Die Lösung Wazuh erfüllt die Anforderungen des Cyberlab am besten. Hier werden alle Funktionen aufgelistet, welche Wazuh gemäss Marketingmaterial von Wazuh Inc., auszeichnen.

Die Software wird als SIEM, sowie als XDR-Lösung vermarktet.
Folgende Use-Cases sind auf der Webseite von Wazuh aufgeführt.

Configuration Assessment

Wazuh kann Konfigurationen der Endpunkte erkennen und mit Regeln abgleichen. Somit werden Events ausgelöst, wenn eine Konfiguration von einer Empfehlung abweicht.

Malware Detection

Wazuh kann helfen, Malware auf Endpunkten zu erkennen, indem «Indicators of Compromise» erkannt werden. Auch die Einbindung von Meldungen von Drittanbieter-Antivirendienstleistungen wie YARA oder Virustotal ist möglich.

File Integrity Monitoring

Wazuh kann erkennen, wenn Dateien geändert oder die Berechtigungen im Dateisystem angepasst werden. Die Benutzer und Applikationen, welche die Datei verändert haben, werden identifiziert.

Threat Hunting

Mithilfe des MITRE ATT&CK Frameworks werden Techniken zum Angriff des Systems identifiziert.

Log Data Analysis

Wazuh kann Logdaten von Endpunkten regelbasiert analysieren. Die Logdaten können mit der «Wazuh Query Language» durchsucht werden.

Vulnerability Detection

Wazuh erstellt ein Software-Inventar von auf Endpunkten installierten Programmen und gleicht diese mit CVEs ab. Bei Treffern wird ein Security Event ausgelöst.

Incident Response

Bei erkannten Angriffen kann Wazuh auch Gegenmassnahmen einleiten, unter anderem das Blockieren von Netzwerkzugriff für den Endpunkt oder die Ausführung von Kommandos auf dem Endpunkt.

Regulatory Compliance

Wazuh kann die Endpunkte mit diversen Compliance-Standards abgleichen und Empfehlungen zur Erreichung der Compliance geben. Insbesondere nennenswert sind NIST 800-53, PCI DSS und die GDPR.

IT-Hygiene

Wazuh bildet ein Inventar aller Endpunkte und zeigt Informationen zu offenen Ports, laufenden Prozessen, installierten Programmen und installierten Betriebssystem-Versionen und Patches.

Containers Security

Wazuh kann auch Container überwachen, wenn es auf dem Containerhost installiert ist.

Posture Management und Workload Protection

Wazuh kann Informationen von Cloud-Anbietern empfangen und helfen, die Compliance im Cloud-Bereich sicherzustellen.

5 Proof of Concept

In diesem Kapitel wird ein Proof of Concept der evaluierten Lösung erstellt und der Vorgang dokumentiert. Dabei werden die Anforderungen aus dem letzten Kapitel berücksichtigt. Zum Schluss werden nötige Schritte zur produktiven Verwendung von Wazuh im Cyberlab dargelegt.

5.1 Systemumgebung

Das Proof of Concept wird im BFH "Cyberlab", welches aktuell in der Entstehung ist, erstellt. Dies bedeutet, dass die Um Systeme möglicherweise ändern können, da immer weitere Systeme in das Cyberlab integriert werden.

5.1.1 Systemzugriff

Das Cyberlab ist nicht grundsätzlich aus dem Internet oder dem BFH-Netzwerk erreichbar. Einzelne Maschinen haben Port-Forwarding auf interne Adressen, was sie erreichbar macht, die allermeisten Systeme sind jedoch hinter einem NAT verborgen.

Um auf das Cyberlab zugreifen zu können, wurde vom Cyberlab-Team ein Wireguard-Tunnel zur Verfügung gestellt.

Tunnel bearbeiten

Name: BFH_Cyberlab

Öffentlicher Schlüssel: tUSlqRtv518rXgLNdCeO3zaF+kk9WYS99GWqnHj7QDw=

```
[Interface]
PrivateKey = 
Address = 10.252.1.120/32
MTU = 1450

[Peer]
PublicKey = 346+cczL6XNatHM5todx7MqGLHZXFWb9ZZLUPxgNzSQ=
PresharedKey = 
AllowedIPs = 192.168.230.0/24
Endpoint = 45.80.137.66:51820
PersistentKeepalive = 15
```

Speichern Abbrechen

Abbildung 7 Konfiguration Wireguard Cyberlab

Gemäss Abbildung der Konfigurationsdatei ist der Wireguard-Server auf der öffentlichen IP-Adresse 45.80.137.66 erreichbar. Einmal im Tunnel eingeloggt, hat der Client die Adresse 10.252.1.120 im Cyberlab Netzwerk.

Für den Zugriff auf die in Kapitel 5.1.2 beschriebenen virtuellen Maschinen wird ein SSH-Key verwendet.

5.1.2 Infrastruktur für Proof of Concept

Für das Proof of Concept wurden vom Team des Cyberlab zwei virtuelle Maschinen bereitgestellt. Ein Gerät wird zum Betreiben eines Wazuh-Clusters verwendet und folgend als «Server» bezeichnet, das andere dient als Client zur Installation des Agenten und wird in der folgenden Tabelle als «Client» bezeichnet.

Die Systemspezifikationen sind folgender Tabelle zu entnehmen.

	Server	Client
Hostname	thesis-siem	thesis-siem-client
IP-Adresse	192.168.230.160	192.168.230.161
# CPU Kerne	4	2
RAM	8 GB	4 GB
Festplatte	50 GB	32 GB
OS-Version	Debian 12	Debian 12

Tabelle 13 Spezifikationen VM Infrastruktur PoC

Für das System «thesis-siem» wurde ein Zertifikat ausgestellt, welches von der internen CA im Cyberlab signiert wurde. Das entsprechende Root-Zertifikat wurde auch ausgehändigt, womit die Zertifizierungskette vervollständigt wird und das System mit einem gültigen Zertifikat gesichert werden kann. Dieses Zertifikat wird für die Einrichtung von TLS gemäss dem Kapitel 5.4 benötigt.

Auf folgenden weiteren Systemen wurde der Wazuh Agent durch das Cyberlab-Team installiert. Auf diese Systeme hat mit Ausnahme des «thesis-siem-client» nur das Cyberlab Team Zugriff.

ID	Hostname	IP-Adresse
001	prometheus	192.168.230.104
002	play-ldap	192.168.230.3
003	test-wireguard	192.168.230.2
004	test-gitea	192.168.230.241
005	test-smallstep-ca	192.168.230.106
006	test-journal	192.168.230.4
007	thesis-siem-client	192.168.230.161

Tabelle 14 Spezifikationen Agent Endpunkte PoC

5.2 Wazuh Architektur

Wazuh hat Agenten auf Endpunkten, welche mit den Serverkomponenten kommunizieren. Im Fall des PoC sind alle Serverkomponenten auf einem einzelnen Server installiert. Falls das System über 100 Endpunkte skalieren soll, ist eine verteilte Installation empfohlen, bei welcher die verschiedenen Serverkomponenten auf eigenen Servern bzw. virtuellen Maschinen installiert werden.

Die Daten der Agenten werden als erstes an den Wazuh Server gesendet, dieser analysiert die Daten und löst bei Bedarf Security Events aus. Die Daten werden dann zur Ablage und Indexierung an den Indexer weitergegeben.

Das Dashboard stellt Daten aus dem Indexer in Dashboards dar. Auch Security Events des Wazuh Servers werden dargestellt, die Konfiguration des Wazuh Servers lässt sich ebenfalls über diese Weboberfläche gemacht werden.

Diese Architektur ist in folgender Grafik anschaulich dargestellt.

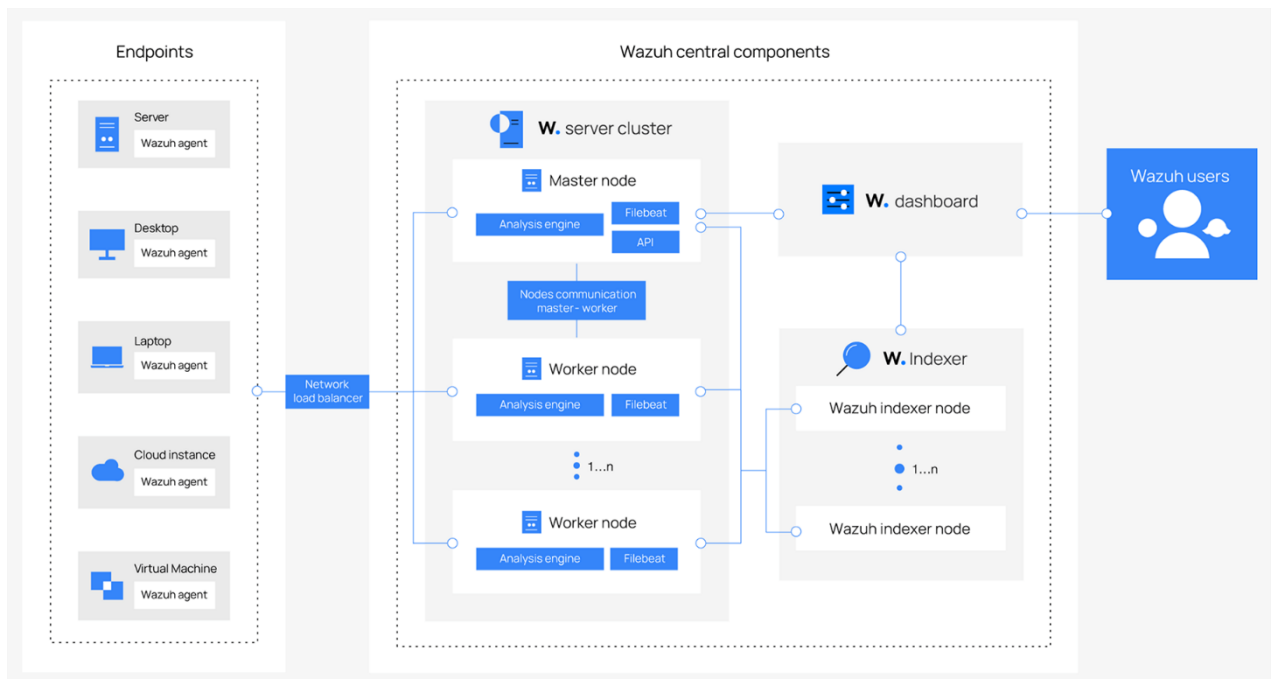


Abbildung 8 Wazuh Architektur

Quelle: <https://wazuh.com/wp-content/themes/wazuh-v3/assets/images/platform/security-platform.png>

Die Komponenten von Wazuh sind in folgender Grafik detailliert aufgeführt.

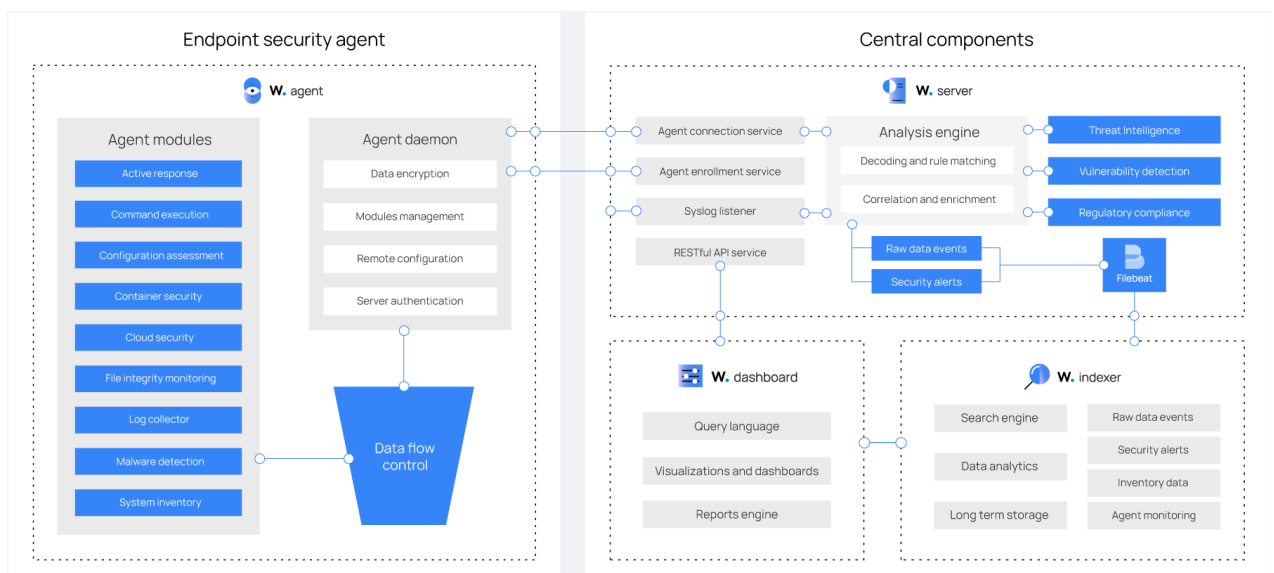


Abbildung 9 Wazuh Komponenten

Quelle: 009_wazuh-components-and-data-flow1.png: https://documentation.wazuh.com/current/_images/wazuh-components-and-data-flow1.png

5.3 Installation Proof of Concept

5.3.1 Wazuh Serverkomponenten

Für die Installation von Wazuh im Proof of Concept wurde das «Quickstart»-Script von Wazuh verwendet. Dies installiert alle nötigen Komponenten für die Serverumgebung auf einem einzelnen Server.

Die Server-Software wird auf dem System «thesis-siem» installiert.

Download des Installationsscripts

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

Installation der Software

```
sudo bash ./wazuh-install.sh -a -i
```

Das Argument “-i” wird benötigt, damit die Überprüfung der empfohlenen Betriebssystem-Version übersprungen (ignoriert) wird.

Das verwendete Debian ist nicht auf der Liste der empfohlenen Systeme.

Aktivieren des Wazuh Agent Dienstes

```
sudo systemctl daemon-reload  
sudo systemctl enable wazuh-agent  
sudo systemctl start wazuh-agent
```

Nach erfolgreicher Installation werden die Zugangsdaten für die Weboberfläche in der Konsole gezeigt.

Unter der IP-Adresse des Servers ist das Wazuh Dashboard ersichtlich, für das Login muss anfangs das vom System selbst signierte Zertifikat für die TLS-Verbindung akzeptiert werden.

Nun kann mit der Installation der Agenten fortgefahren werden

5.3.2 Wazuh Agent

Der Agent wird auf dem Endpunkt direkt von Wazuh heruntergeladen und installiert. Im Falle einer x86 Linux-VM sieht die Installation folgendermassen aus.

Download des Pakets

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb
```

Agent Installation

```
sudo WAZUH_MANAGER='192.168.230.160' dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb
```

Zur Installation muss die Umgebungsvariable «WAZUH_MANAGER» mit der Adresse des Servers befüllt werden.

Nach erfolgreicher Installation sind die Daten des Endpunktes im Wazuh Dashboard ersichtlich.

Für das Proof of Concept wurde dies auf den Maschinen aus der Tabelle «Tabelle 14» durchgeführt. Auf den Maschinen ausser «thesis-siem-client» wurde die Agent-Installation durch das Team des Cyberlab durchgeführt, da für die Thesis keine Shell-Zugriff auf die anderen Maschinen im Netzwerk gewährt wurde.

Spezialfall Agent auf LXC-Containern

Manche Systeme im Cyberlab laufen in LXC-Containern. In diesen wurde die benötigte Environment-Variable «WAZUH_MANAGER» nicht übernommen.

Damit der Agent trotzdem funktioniert, muss dort die Konfigurationsdatei «/var/ossec/etc/ossec.conf» angepasst und der Wert des Knotens «address» auf die IP-Adresse des Wazuh-Servers gesetzt werden.

5.3.3 E-Mail-Benachrichtigungen

Wazuh kann Benachrichtigungen per E-Mail versenden, sobald Alerts eines bestimmten Levels auftreten.

Dies wird in der Konfigurationsdatei «/var/ossec/etc/ossec.conf» konfiguriert. Der folgende ausschnitt zeigt die angepassten Parameter, dieser Konfiguration.

```
<global>
  <jsonout_output>yes</jsonout_output>
  <alerts_log>yes</alerts_log>
  <logall>no</logall>
  <logall_json>no</logall_json>
  <email_notification>yes</email_notification>
  <smtp_server>mail.nslab.ch</smtp_server>
  <email_from>wazuhserver@nslab.ch</email_from>
  <email_to>wazuh@nslab.ch</email_to>
  <email_maxperhour>12</email_maxperhour>
  <email_log_source>alerts.log</email_log_source>
  <agents_disconnection_time>10m</agents_disconnection_time>
  <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
</global>

<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>3</email_alert_level>
</alerts>
```

Im Teil «global» werden E-Mail-Server, Absender und Empfänger konfiguriert, sowie die maximale Anzahl E-Mails pro Stunde definiert.

Für Testzwecke ist ein niedriger Wert hier von Vorteil, um nicht hunderte E-Mails von Alerts ein Posteingang zu haben.

Für eine produktive Umgebung besteht bei einem zu niedrigen Wert die Gefahr, Benachrichtigungen zu verlieren.

Wazuh geht standardmässig von einer Verbindung ohne Authentifizierung aus und kann von Haus aus auch keine Verschlüsselung beim E-Mail-Transport anbieten.

E-Mail-Konfiguration BFH Cyberlab

Der E-Mail-Server «mail.nslab.ch» wurde so konfiguriert, dass E-Mails an die Adresse «wazuh@nslab.ch» automatisch an eine vorkonfigurierte E-Mail-Adresse der BFH weitergeleitet werden.

Wazuh kann so E-Mails via diesen Mailserver an eine E-Mail-Adresse der BFH versenden.

5.4 Sicherheitsaspekte

Aus den Sitzungen mit dem Cyberlab-Team ist hervorgegangen, dass Sicherheitsaspekte für das Projekt wichtig sind. Die Verwendung einer Host-Firewall ist wünschenswert und der Datenaustausch soll verschlüsselt erfolgen.

5.4.1 Verschlüsselte Kommunikation

Die Kommunikation von Wazuh darf grundsätzlich nur verschlüsselt erfolgen.

Mit dem Quickstart-Paket wird dies Out-of-the-Box gewährleistet, da von Wazuh selbst signierte Zertifikate für die Kommunikation über TLS verwendet werden.

Für das Wazuh-Dashboard wird ebenfalls ein selbst signiertes Zertifikat verwendet, was dazu führt, dass der Browser eine Warnung wegen eines nicht-vertrauenswürdigen Zertifikates ausgibt. Vom Cyberlab-Team wurde neben der virtuellen Maschine «thesis-siem» auch ein Zertifikat für die Namen «thesis-siem.clab.playground», «thesis-siem» und «192.168.230.160» mitgegeben. Dies wurde von der internen CA im Cyberlab erstellt. Das entsprechende CA-Zertifikat wurde auch mitgegeben.

Das Wazuh Dashboard wurde so konfiguriert, dass es dieses TLS-Zertifikat ausliefert. Ist das entsprechende CA-Zertifikat im Browser installiert, werden keine Warnungen mehr bezüglich nicht-vertrauenswürdiger Zertifikate generiert.

Zur einfachen Erreichung dieses Ziels wird ein nginx-Reverse-Proxy eingesetzt. Die Funktionsweise ist in folgender Grafik illustriert.

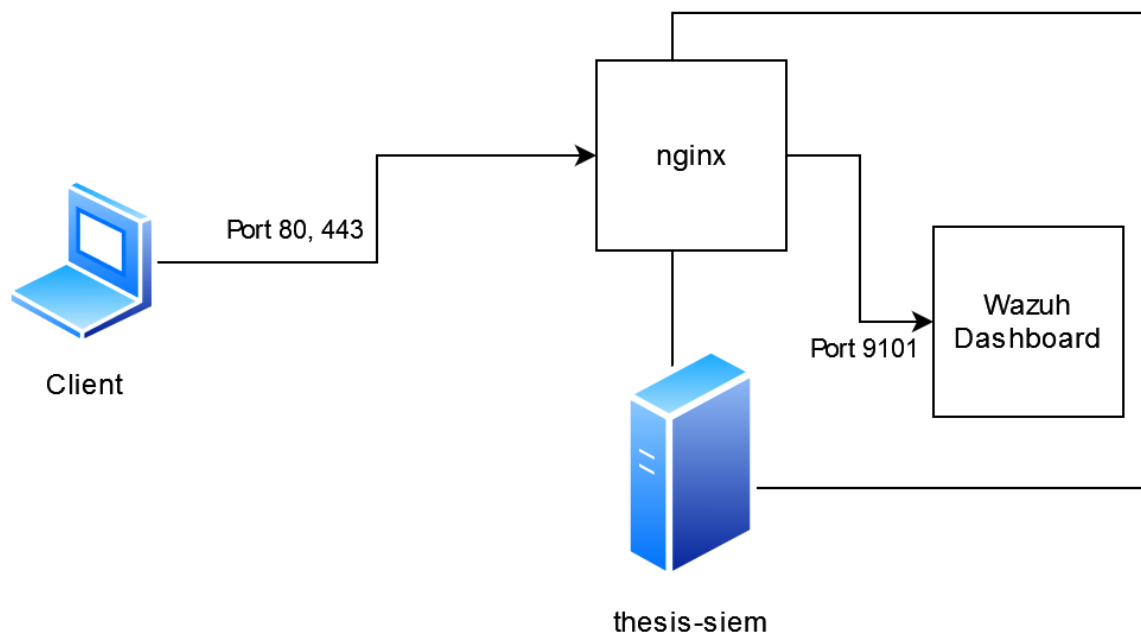


Abbildung 10 Diagramm nginx Reverse Proxy Wazuh

Der Wazuh-Dashboard Dienst, welcher normalerweise auf Port 443 hört, wird auf einen anderen Port verschoben, stattdessen hört ein nginx Webserver auf Port 443 und in diesem Fall auch auf Port 80 für eine einfache Umleitung auf Port 443.

Installation nginx

```
sudo apt install nginx
```

Der Webserver nginx wird einfach vom Debian Repository installiert.

Konfiguration nginx

Die Konfigurationsdatei, welche unter «/etc/nginx/sites-available/wazuh-dashboard-proxy» erstellt wurde, ist im Anhang mit der Kapitelnummer 12.5 zu finden.

Sie enthält zwei virtuelle Webserver, einer hört auf Port 80 und leitet auf den Server, welcher auf Port 443 hört, um.

Dieser wiederum ist für TLS, mit dem vom Cyberlab Team bereitgestellten TLS-Zertifikat konfiguriert und leitet alle Anfragen an das Wazuh-Dashboard auf Port 9101 weiter.

Für den Zugriff auf nginx muss der Webserver-Benutzer in der Gruppe «ssl-access» sein.

```
sudo usermod -a -G ssl-access www-data
```

Aktivierung nginx

Die Konfiguration des Reverse-Proxys muss noch aktiviert werden, dazu die Datei nach «sites-enabled» verlinken und nginx neu laden.

```
sudo ln -s /etc/nginx/sites-available/wazuh-dashboard-proxy /etc/nginx/sites-enabled/wazuh-dashboard-proxy
```

Prüfung, ob Konfiguration von nginx ok ist. Falls Fehler vorhanden sind, wird die entsprechende Zeilennummer ausgegeben.

```
sudo nginx -t
```

Den nginx Dienst neustarten und den Status kontrollieren.

```
sudo systemctl restart nginx
```

```
sudo systemctl status nginx
```

5.4.2 Host Firewall

Für die Host-Firewall wurde «nftables» verwendet. Die Konfiguration wurde so erstellt, dass nur vordefinierte Ports für eingehende Verbindungen geöffnet sind, alle anderen eingehenden Verbindungen werden verworfen. Ausgehende Verbindungen werden grundsätzlich erlaubt. Pakete, welche den Host nur traversieren (Routing) werden verworfen. Datenverkehr auf dem Loopback-Interface wird grundsätzlich erlaubt.

Komponente	Port	Protokoll	Nutzen
Wazuh Server	1514	TCP	Verbindung zu Agenten
	1514	UDP	Verbindung zu Agenten (optional)
	1515	TCP	Agentenregistrierung
	1516	TCP	Wazuh Clustering
	514	UDP	Syslog Kollektor (optional)
	514	TCP	Syslog Kollektor (optional)
	5500	TCP	Wazuh Server REST API
Wazuh Indexer	9200	TCP	Wazuh Indexer REST API
	9300 - 9400	TCP	Wazuh Indexer Cluster Kommunikation
Wazuh Dashboard	80, 443	TCP	Wazuh Web Interface

Tabelle 15 Portliste Wazuh

Quelle: <https://documentation.wazuh.com/current/getting-started/architecture.html>

Installation nftables

```
sudo apt install nftables
```

Konfiguration nftables

Die Konfigurationsdatei «/etc/nftables» wurde mit Regeln zum Whitelisting der nicht-optionalen Ports aus Tabelle 15 ergänzt. Auch Port 22/TCP für den Zugriff per SSH und schon bestehende Verbindungen wurden erlaubt.

Die Konfigurationsdatei ist in Anhang mit der Kapitelmarke **Error! Reference source not found.** abgelegt.

Konfiguration aktivieren

```
sudo systemctl enable nftables
```

Damit wurde die Firewall aktiviert.

5.5 Zielabdeckung Proof of Concept

Die in den Kapiteln 4.3.1 und 4.3.2 definierten Ziele an das Produkt und die Umsetzung werden hier auf ihren Erreichungsgrad überprüft.

5.5.1 Methodik

Die Zielabdeckung der Anforderungen an das SIEM und der Anforderungen an die Umsetzung werden separat in einem jeweils eigenen Unterkapitel überprüft. Zur Überprüfung wird jeder Anforderung in einer Tabelle aufgeführt und mit einer der drei Möglichkeiten «erfüllt», «teilweise erfüllt» oder «nicht erfüllt» bewertet.

Die entsprechende Tabelle sieht folgendermassen aus.

Nr.	Beschreibung	Erfüllungsgrad
T1	Testweise Anforderung 1	erfüllt
T2	Testweise Anforderung 2	teilweise erfüllt

Tabelle 16 Vorlage Überprüfung Zielabdeckung PoC

Pro Anforderung wird danach im Detail beschrieben, wie die Bewertung zustande kommt.

5.5.2 Überprüfung Anforderungen an das SIEM

Dieses Kapitel beschreibt die Erfüllung der Anforderungen das Proof of Concept mit Wazuh.

Nr.	Beschreibung	Erfüllungsgrad
A1	Open Source Lizenz	erfüllt
A2	Wird noch aktiv weiterentwickelt	erfüllt
A3	Erfüllt Kriterien eines SIEM	erfüllt
A4	Erkennung von Security Events	erfüllt
A5	Alarmierung bei Security Events	erfüllt
A6	Alarmierung nur bei Security Incidents (Unterscheidung zu Events)	teilweise erfüllt
A7	Daten für Dashboard bereitstellbar	erfüllt
A8	Lösung bietet ein ausführliches Dashboard	erfüllt
A9	Aktive Komponenten (Möglichkeit auf Incidents zu reagieren)	erfüllt

Tabelle 17 PoC Überprüfung Zielabdeckung SIEM

A1 Open Source Lizenz

Das Produkt ist unter GNU GPL v2 und der Apache License 2.0 lizenziert. Beide Lizenzen sind von der Open Source Initiative anerkannt.

A2 Wird noch aktiv weiterentwickelt

Wazuh hat eine aktive Community und wird weiterentwickelt.

A3 Erfüllt Kriterien eines SIEM

Wazuh erfüllt die Anforderungen an ein SIEM gemäss Kapitel 2.2.

A4 Erkennung von Security Events

Wazuh kann Security Events erkennen, die Regeln dafür sind bei der Installation von Wazuh dabei und schon aktiv. Natürlich können sie beliebig erweitert werden. Events werden in einer Übersicht dargestellt.

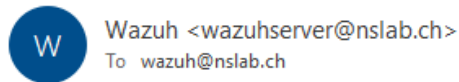
Security Alerts							
	Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level
>	May 7, 2024 @ 14:48:10.870	007	thesis-siem-client			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 14:48:10.844	007	thesis-siem-client			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:40:30.322	001	prometheus			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:40:30.294	001	prometheus			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:38:35.950	003	test-wireguard			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:38:35.931	003	test-wireguard			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:38:35.910	003	test-wireguard			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:38:35.890	003	test-wireguard			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:38:35.870	003	test-wireguard			Host-based anomaly detection event (rootcheck).	7
>	May 7, 2024 @ 13:38:35.850	003	test-wireguard			Host-based anomaly detection event (rootcheck).	7

Abbildung 11 PoC Wazuh Security Events

A5 Alarmierung bei Security Events

Eine Alarmierung bei Security Events ist möglich und im Proof of Concept auch umgesetzt. Die Alarmierung ist so eingerichtet, dass bei Events, welche ein Level überschreiten, eine E-Mail-Benachrichtigung ausgelöst wird.

Wazuh notification - (thesis-siem-client) any - Alert level 3



Wazuh Notification.
2024 May 07 18:33:06

Received From: (thesis-siem-client) any->wazuh-remoted
Rule: 506 fired (level 3) -> "Wazuh agent stopped."
Portion of the log(s):

ossec: Agent stopped: 'thesis-siem-client->any'.

--END OF NOTIFICATION

Abbildung 12 PoC Wazuh Security Event-E-Mail

A6 Alarmierung nur bei Security Incidents (Unterscheidung zu Events)

Die Unterscheidung von Events zu Incidents kann durch granulare Regeln zur Klassifizierung von Security Events zu einem grossen Teil automatisiert werden. Die definitive Entscheidung kann jedoch nicht durch das System getroffen werden.

A7 Daten für Dashboard bereitstellbar

Die indexierten Daten sind auf Port 9200/TCP vom Wazuh Indexer über eine REST-API abfragbar. Echtzeit-Events könnten mit einer REST-API auf Port 55000/TCP abgefragt werden. Damit bietet Wazuh Daten für die weitere Verwendung in Dashboards oder eigener Software an. Die Nutzung des internen Dashboards ist jedoch komfortabler.

A8 Lösung bietet ein ausführliches Dashboard

Das Wazuh Dashboard bietet die Möglichkeit, komplexere Dashboards zu erstellen. Gerade für die Darstellung von Security Events muss jedoch die Archivierung von Security-Events aktiviert werden, dies passiert nicht standardmässig. Dazu muss die Variable «logall_json» in der Konfigurationsdatei «/var/ossec/etc/ossec.conf» auf «yes» gesetzt und der Wazuh-Dienst mit «systemctl restart wazuh-manager» neugestartet werden.

A9 Aktive Komponenten (Möglichkeit auf Incidents zu reagieren)

Wazuh kann auf Incidents nicht nur per E-Mail, sondern auch mit automatisierten Gegenmassnahmen reagieren. So können auf dem Zielsystem bei Registrierung eines Events, Scripts ausgeführt und so zum Beispiel eine Firewall-Regel angepasst werden.

5.5.3 Überprüfung Anforderungen an die Umsetzung

Dieses Kapitel beschreibt die Erfüllung der Anforderungen an die Umsetzung des Proof of Concept.

Nr.	Beschreibung	Erfüllungsgrad
U1	Konfigurationen sind nachvollziehbar	erfüllt
U2	Das System ist einfach reproduzierbar	erfüllt
U3	Security Considerations werden angestellt	erfüllt
U4	Die Konfigurationsphilosophie des BFH Cyberlab wird eingehalten	teilweise erfüllt

Tabelle 18 PoC Überprüfung Zielabdeckung Umsetzung

U1 Konfigurationen sind nachvollziehbar

Alle Konfigurationen, welche für die Erstellung des PoC nötig sind, sind im Kapitel 5.3 dokumentiert. Wo nötig wird auf eine Konfigurationsdatei im Anhang verwiesen.

U2 Das System ist einfach reproduzierbar

Mittels Dokumentation aus Kapitel 5.3 kann das gesamte PoC nachgebaut werden. Bei Bedarf kann aus dieser Dokumentation ein Ansible-Script erstellt werden.

U3 Security Considerations werden angestellt

Das Kapitel 5.4 beschreibt die angestellten Security Considerations und wie sie im PoC umgesetzt wurden.

U4 Die Konfigurationsphilosophie des BFH Cyberlab wird eingehalten

Die Secure-Defaults liessen sich grösstenteils umsetzen, einzig der standardmässige Versand von E-Mails erfolgt ohne Authentifizierung über ein E-Mail-Relais.

Wazuh bietet zur Konfiguration keine Drop-In-Ordner an, wo Konfigurationen in separate Dateien geschrieben werden könnten. Es mussten also Konfigurationsdateien angepasst werden.

5.6 Konzept zur Überführung in produktiven Betrieb

Um das erarbeitete Proof of Concept in den produktiven Betrieb zu überführen, müssen einige Punkte beachtet werden.

5.6.1 Skalierung

Das Proof of Concept wurde als Single-Host-Installation erstellt. Gemäss Wazuh-Dokumentation skaliert diese Installationsart bis 100 Endpunkte.

Um dies zu erreichen sind 8 CPU-Kerne, 8GB RAM, sowie 200 GB Speicherplatz notwendig.

Theoretisch können einer virtuellen Maschine auch noch mehr Ressourcen zugewiesen werden, die Empfehlung der Wazuh-Dokumentation besagt aber, dass die Installation zur weiteren Skalierung aufgeteilt werden soll.

Die Wazuh- und Indexer-Server können auch im Clusterbetrieb laufen, es können also mehrere Instanzen laufen und für die gleiche Wazuh Installation arbeiten. So skaliert Wazuh für weitere Endpunkte.

Es ist zu vermuten, dass eine Limitation in der Software-Architektur dazu führt, dass weitere Ressourcen nicht mehr effizient skalieren und die Arbeit so auf weitere Instanzen verteilt werden muss. Es spricht in einem Lab aber nichts dagegen, die Skalierung der Single-Host-Installation durch Zuweisung weiterer Ressourcen, also vertikale Skalierung, zu testen.

Ob Wazuh an seine Grenzen kommt, kann überprüft werden, indem die Variable «events_dropped» in der Datei «/var/ossec/var/run/wazuh-analysisd.state» untersucht wird. Diese zählt wie viele Events aufgrund mangelnder Ressourcen verworfen werden.

Die Variable «discarded_count» in der Datei «/var/ossec/var/run/wazuh-remoted.state» macht dasselbe für ganze Agenten. Sie zeigt also auf, ob Agenten aufgrund fehlender Ressourcen ignoriert werden müssen.

Beide Werte sollen in einer gesunden Wazuh-Installation «0» sein.

5.6.2 Installation der Endpunkte

Der Wazuh Agent wird auf Linux-Systemen als einfaches Paket installiert, dies ist im Kapitel 5.3.2 beschrieben.

Diese Installation sollte für Maschinen im Cyberlab automatisiert werden. Entweder als Teil eines Ansible-Scripts oder mit einer anderen Möglichkeit zum Verteilen von Software in Systemumgebungen.

Die Anzahl Windows-Geräte ist nach aktueller Planung überschaubar, weshalb hier eine manuelle Installation noch in Frage kommt. Bei Bedarf muss auch hier eine Möglichkeit zur automatischen Installation des Agenten gefunden werden.

5.6.3 Konfiguration der Alerts

In der Konfigurationsdatei `«/var/ossec/etc/ossec.conf»` sollte das Alert-Level angepasst werden, bei welchem ein E-Mail-Alert versendet wird. Dazu kann die Variable `«email_alert_level»` auf einen Wert zwischen 1 und 12 gesetzt werden, wobei 1 das niedrigste und 12 das höchste Alert-Level ist. Niedrige Werte generieren entsprechend mehr E-Mail-Benachrichtigungen.

Auch die E-Mail-Konfiguration kann überdacht werden, es ist empfehlenswert eine Adresse eines geteilten E-Mail-Postfachs für die Benachrichtigungen von Wazuh Alerts zu verwenden.

Falls die Alerts für weitere Analysen gespeichert werden sollen, muss dies in der Konfiguration eingeschaltet werden.

Dazu muss die Variable `«logall_json»` in der Konfigurationsdatei `«/var/ossec/etc/ossec.conf»` auf `«yes»` gesetzt und der Wazuh-Dienst mit `«systemctl restart wazuh-manager»` neugestartet werden.

5.6.4 Dashboards

Für den produktiven Betrieb können Dashboards zur Darstellung diverser Eckdaten der Systemumgebung erstellt werden. Diese sind dann über das Wazuh-Dashboard zugänglich. Die Konfiguration der Dashboards ist ähnlich zur Konfiguration von Kibana-Dashboards, da «OpenSearch» verwendet wird, was ein Fork von Kibana aus dem Elastic-Stack ist.

5.6.5 Benutzerverwaltung

Für den produktiven Betrieb machen verschiedene Benutzer mit entsprechenden Berechtigungen Sinn. Diese sind im Front-End im Bereich «Security» konfigurierbar.

So können Benutzer erstellt werden, welche dann nur Zugriff auf die Dashboards haben. So wird das Risiko durch gespeicherte Anmeldedaten z.B. für PCs an Bildschirmen an öffentlich zugänglichen Orten verringert. Diese Benutzer können dann keine Konfigurationsänderungen machen.

5.6.6 Betrieb

Für den Betrieb von Wazuh sind grundsätzlich dieselben Überlegungen wie für den Betrieb anderer Software notwendig.

Die Maschine sollte immer aktuell gehalten werden, dies ist im Cyberlab gegeben, da Debian-Server hier automatisch Updates installieren.

Die Ressourcenausnutzung gilt es zu kontrollieren, vor allem die Verwendung von Festplattenplatz ist bei der Speicherung von Event vieler Endpunkte relevant. Es könnte mehr Platz benötigt werden.

6 Schlussfolgerungen/Fazit

Dieser Teil der Arbeit beschreibt die erzielten Ergebnisse und untersucht die in Kapitel 1.2 definierten Ziele auf ihre Erfüllung

Ein persönliches Fazit und ein Ausblick auf mögliche Weiterführungen der Arbeit in weiteren Projekten schliessen die Arbeit ab.

6.1 Zielerreichung

Zur Überprüfung der Zielerreichung der Projektziele wird eine ähnliche Methodik verwendet, welche auch zur Überprüfung der «Proof of Concept»-Ziele verwendet wurde. Die Methode ist im Kapitel 5.5.1 beschrieben.

Der Hauptunterschied ist, dass pro Ziel auch die Kapitel der Dokumentation angegeben sind, welche zur Erfüllung erstellt wurden.

Nr.	Beschreibung	Erfüllungsgrad	Kapitel
M1	Der Bericht enthält eine Einführung in «SIEM»	erfüllt	2
M2	Der Bericht enthält eine Marktübersicht über SIEM-Lösungen	erfüllt	3
M3	Die Anforderungen an die SIEM-Lösung für Laborumgebungen wurden aufgenommen	erfüllt	4.3
M4	Eine Evaluation der SIEM-Lösung für Laborumgebungen wurde durchgeführt	erfüllt	4.4
M5	Ein Proof of Concept der evaluierten Lösung wurde erstellt	erfüllt	5
M6	Die Anforderungen aus Ziel «M3» wurden mit dem PoC aus Ziel «M5» abgeglichen	erfüllt	5.5
M7	Der Bericht enthält einen Vorschlag zur Überführung des PoC aus Ziel «M6» in den produktiven Betrieb	erfüllt	5.6

Tabelle 19 Zielüberprüfung "Muss"

Die Arbeit konnte alle Muss-Ziele abdecken und erfüllen. Sie beginnt mit einer Einführung in die Thematik SIEM und beschreibt, welche Eigenschaften ein SIEM haben muss. Die Marktübersicht gibt Auskunft über aktuelle Angebote im Bereich SIEM und stellt die Grundlage für die spätere Evaluation dar.

Vor der Evaluation wurden die Anforderungen an das SIEM in einem Gespräch mit dem Cyberlab-Team aufgenommen. Diese Anforderungen wurden anschliessend in einer Evaluation verwertet und das passende Produkt «Wazuh» gefunden.

Weiter aufbauend auf allen vorherigen Erkenntnissen wurde das Proof of Concept mit Wazuh im Cyberlab umgesetzt und die vorherigen Anforderungen mit dem entstandenen Proof of Concept abgeglichen. Dieser Abgleich befand, dass alle bis auf zwei Ziele des Proof of Concept erfüllt wurden, wobei ein Ziel teilweise und ein anderes nicht erfüllt wurde.

Um aus dem entstandenen Proof of Concept ein produktionsreifes System für das BFH Cyberlab zu machen, wurden die nötigen Überlegungen im Kapitel 5.6 festgehalten.

Nr.	Beschreibung	Erfüllungsgrad	Kapitel
K1	Der Bericht enthält eine Erklärung des IDMEF (Intrusion Detection Message Exchange Format)	erfüllt	2.3
K2	Die Marktübersicht aus Ziel «M2» enthält eine Übersicht von Produkten, welche sich als SIEM-Bezeichnen, aber nicht unter die Definition fallen	erfüllt	3.3
K3	Die PoC-Lösung aus Ziel «M6» wurde in eine produktionsreife Lösung umgebaut	nicht erfüllt	-

Tabelle 20 Zielüberprüfung "Kann"

Während alle Muss-Ziele erfüllt wurden, ist dies bei den Kann-Zielen nicht ganz der Fall. Eine Einführung in das IDMEF wurde erstellt und der Einführung in SIEM angehängt. Auch das Ziel K2 wurde durch Ergänzung der Marktübersicht mit einem Unterkapitel erfüllt. Hier wurden Systeme, bei welcher die Kategorisierung als SIEM fragwürdig erscheint, genauer untersucht, mit dem Ergebnis, dass zwei von drei untersuchten Systemen nicht in die Kategorie eines SIEM nach Kapitel 2.2 gehören. Eine produktionsreife Lösung wurde während der Arbeit mangels Zeit nicht umgesetzt. Dies ist in Zukunft durch das Laborteam des Cyberlab jedoch möglich, da das Proof of Concept und das dazugehörige «Konzept zur Überführung in den produktiven Betrieb» eine solide Grundlage dafür bieten.

6.2 Learnings und persönliches Fazit

Während der Arbeit habe ich mich mit dem Thema SIEM befasst und mich so in ein neues Thema einarbeiten können. Einige Vorkenntnisse zu Monitoring-Systemen aus der Project 2-Arbeit konnte ich anwenden, SIEM selbst waren mir bis zum Beginn der Arbeit nur oberflächlich bekannt. Ich habe viel über diese Systeme erfahren und mein Wissen beim Untersuchen der am Markt vorhandenen Systeme nutzen können.

Die Erstellung des Proof of Concept hat mir sehr grossen Spass gemacht, da ich mich in der Welt der Systemadministration wohl fühle. Die Installation und Konfiguration hat funktioniert und liess sich entsprechend gut dokumentieren.

Im Verhältnis haben die Recherche, Dokumentation und weitere Schriftliche Arbeitsteile einen grossen Teil dieser Arbeit ausgemacht, wobei die Implementierung des Proof of Concept einen kleineren Teil dargestellt hat. Ich finde aber, dass die praktischen und theoretischen Komponenten zusammenpassen und ein realistisches Bild von SIEM für Laborumgebungen geben.

Persönlich habe ich gelernt mit dem Druck einer so umfangreichen und bedeutenden Arbeit umzugehen und die Arbeit gut auf das ganze Semester zu verteilen.

6.3 Ausblick

Diese Arbeit hat den Grundstein für die Implementation eines SIEM im BFH-Cyberlab gelegt. Nach meiner Empfehlung soll dieses SIEM «Wazuh» sein und gemäss der Dokumentation des PoC und «Überführung in den produktiven Betrieb» in den produktiven Betrieb genommen werden. In weiteren Schritten können möglichst viele Datenquellen angebunden und Aussagekräftige Dashboards erstellt werden.

Das SIEM soll so einen zentralen Überblick über die Labor-Infrastruktur geben können und neben dem Laborteam auch Besucherinnen und Besuchern mit unterschiedlichem Vorwissen einen spannenden Einblick in die Welt der IT-Security geben.

7 Abbildungsverzeichnis

Abbildung 1 Diagramm SIEM Datenquellen	6
Abbildung 2 Zusammenhang Event und Incident	6
Abbildung 3 Diagramm SIEM Aufbau	7
Abbildung 4 Diagramm SIEM Aufbau intern	8
Abbildung 5 Grafik SIM vs. SEM vs. SIEM	9
Abbildung 6 IDMEF Schema	10
Abbildung 7 Konfiguration Wireguard Cyberlab	24
Abbildung 8 Wazuh Architektur	26
Abbildung 9 Wazuh Komponenten	26
Abbildung 10 Diagramm nginx Reverse Proxy Wazuh	29
Abbildung 11 PoC Wazuh Security Events	32
Abbildung 12 PoC Wazuh Security Event-E-Mail	33

8 Tabellenverzeichnis

Tabelle 1 Zieldefinition "Muss"	4
Tabelle 2 Zieldefinition "Kann"	4
Tabelle 3 IDMEF Heartbeat Inhalt	10
Tabelle 4 IDMEF Alert Inhalt	11
Tabelle 5 Beschreibung Bewertungskriterien	13
Tabelle 6 Vorlage Marktübersicht	13
Tabelle 7 Marktübersicht SIEM	14
Tabelle 8 Vorlage Anforderungen	18
Tabelle 9 Anforderungen an das System	18
Tabelle 10 Anforderungen an die Umsetzung	19
Tabelle 11 Bewertung Anforderungen SIEM	21
Tabelle 12 Resultate SIEM Bewertung	22
Tabelle 13 Spezifikationen VM Infrastruktur PoC	25
Tabelle 14 Spezifikationen Agent Endpunkte PoC	25
Tabelle 15 Portliste Wazuh	31
Tabelle 16 Vorlage Überprüfung Zielabdeckung PoC	31
Tabelle 17 PoC Überprüfung Zielabdeckung SIEM	32
Tabelle 18 PoC Überprüfung Zielabdeckung Umsetzung	34
Tabelle 19 Zielüberprüfung "Muss"	36
Tabelle 20 Zielüberprüfung "Kann"	36

9 Abkürzungsverzeichnis

EDR	
Endpoint Detection and Response	5
IDS	
Intrusion Detection System	5
IPS	
Intrusion Prevention System	5
PoC	
Proof of Concept	5
SEM	
Security Event Management	5
SIEM	
Security Information and Event Management	5
SIM	
Security Information Management	5
XDR	
Extended Detection and Response	5

10Glossar

Dieses Verzeichnis referenziert die Seitenzahl der Kapitelüberschrift, in wessen Kapitel der Begriff verwendet wird.

Cyber Killchain	
Kette von Ereignissen, welche zu Cybervorfall führen	5
Proof of Concept	
Versuch, ein Produkt zu erstellen oder zu verwenden um ein Ziel zu erreichen	5
Endpoint Detection and Response	
Software um Schutz von Geräten sicherzustellen	5
Intrusion Detection System	
System zur Erkennung von Eindringungsversuchen in Netzwerke oder Systeme	5
Intrusion Prevention System	
System zur Erkennung und Bekämpfung von Eindringungsversuchen in Netzwerke oder Systeme	5
Security Event Management	
System zur Erkennung und Alarmierung bei Security Events, siehe Kapitel 2.2	5
Security Information Management	
System zur Analyse von Logs und Erkennung von Security Events, siehe Kapitel 2.2	5
Security Information and Event Management	
Kombination von SIM und SEM, siehe Kapitel 2.2	5
Extended Detection and Response	
Software um umfassenden Schutz von Geräten und deren Umgebung zu gewährleisten	5
Heartbeat	
Regelmässiger Austausch von Information zur Sicherstellung ein Verbindung	10
Security Event	
Ein Ereignis, welches möglicherweise eine Auswirkung auf ein System hat	18
Security Incident	
Ein Security Event, welches zu einer Auswirkung auf ein System geführt hat	18

11 Literaturverzeichnis

Dieses Verzeichnis referenziert die Seitenzahl der Kapitelüberschrift, in wessen Kapitel die Quelle verwendet wird.

Aufgabenstellung Bachelorthesis

Wenger, Hansjürg, P24-Trachsel.pdf,
https://moodle.bfh.ch/pluginfile.php/2936046/mod_folder/content/0/P24-Trachsel.pdf, 2024 4

Was SIM und SEM von SIEM unterscheidet

<https://www.computerwoche.de/a/was-sim-und-sem-von-siem-unterscheidet>, 25.11.2013, 2013 5

Security Incident vs Event

<https://www.bitlyft.com/resources/security-incident-vs-event-what-is-the-difference>, 2019 5

Information Security BTI4204

Wenger, Hansjürg, S24.01 - Information Security.pdf, Unterlagen BTI4204, 2023 5

A Brief History of SIEM

<https://cybersecurity-magazine.com/a-brief-history-of-siem/>, 2020 5

Security Information and Event Management (SIEM)

<https://www.michaelgorski.net/soc-siem-beratung/siem-beratung/security-information-and-event-management-siem/>, abgerufen: 2024 5

Video: Wozu braucht man ein SIEM?

Dr. Michael Gorski – IT-Security, <https://youtu.be/QYiOTOpdknU>, 2020 5

Video: SIEM was ist das? (Security Information and Event Management)

Dr. Michael Gorski – IT-Security, <https://youtu.be/httNmeYtR10>, 2021 5

Draw.io Editor Diagrammerstellung

<https://www.drawio.com/>, abgerufen: 2024 6, 7, 8, 29

Gartner SIEM Reviews and Ratings

<https://www.gartner.com/reviews/market/security-information-event-management>, abgerufen: 2024 12

Geekflare 11 Best SIEM Tools

<https://geekflare.com/best-siem-tools/>, 2023 12

Geekflare 7 Best Open Source SIEM Systems

<https://geekflare.com/best-open-source-siem-systems/>, 2023 12

IETF RFC4765 IDMEF

<https://www.ietf.org/rfc/rfc4765.txt>, 2007 10

Wikipedia IDMEF

https://en.wikipedia.org/wiki/Intrusion_Detection_Message_Exchange_Format, 2020 10

Github IDMEFv2

<https://github.com/IDMEFv2/>, 2024 10

AlienVault OSSIM

<https://cybersecurity.att.com/products/ossim>, abgerufen: 2024 14, 15

Elastic Stack-Abonnements

<https://www.elastic.co/de/subscriptions>, abgerufen: 2024 14, 21

Graylog V4.0 Licensing SSPL

<https://graylog.org/post/graylog-v4-0-licensing-sspl/>, abgerufen: 2024 14, 21

IBM Security QRadar Pricing

<https://www.ibm.com/products/qradar-siem/pricing>, abgerufen: 2024 14

LogRhythm SIEM Licensing

<https://docs.logrhythm.com/lrsiem/7.13.0/licensing>, abgerufen: 2024 14

OSSEC Wikipedia

<https://en.wikipedia.org/wiki/OSSEC>, abgerufen: 2024 14

Github Prelude-SIEM

<https://github.com/Prelude-SIEM/Prelude-SIEM>, abgerufen: 2024 14

Prelude OSS Project	
https://www.prelude-siem.org/ , abgerufen: 2024	14
Splunk Community Difference Enterprise and Enterprise Security	
https://community.splunk.com/t5/Splunk-Enterprise-Security/What-is-the-difference-between-Splunk-Enterprise-and-Splunk/m-p/434194 , 2018	14
Github Wazuh License	
https://github.com/wazuh/wazuh/tree/master?tab=License-1-ov-file#readme , 2022	14, 20
Snort	
https://www.snort.org/ , abgerufen: 2024	15
SolarWinds SEM	
https://www.solarwinds.com/security-event-manager , abgerufen: 2024	15
OSSEC	
https://www.ossec.net/ , abgerufen: 2024	21
Wazuh	
https://wazuh.com/ , abgerufen: 2024	21, 23, 27
Wazuh Guide	
https://documentation.wazuh.com/current/quickstart.html , abgerufen: 2024	24
Schriftverkehr Cyberlab Team	
Schrag, Kevin, E-Mail: Re: Installation Wazuh Agent, Verlag, 15.04.2024	27
Wazuh Architektur Liste mit Ports	
https://documentation.wazuh.com/current/getting-started/architecture.html , abgerufen: 2024	31
Wazuh E-Mail bei Alerts	
https://documentation.wazuh.com/current/user-manual/manager/manual-email-report/index.html , abgerufen: 2024	28
Wazuh NGINX Reverse Proxy	
https://documentation.wazuh.com/current/user-manual/wazuh-dashboard/configuring-third-party-certs/ssl-nginx.html , abgerufen: 2024	29
nftables Manual	
https://wiki.archlinux.org/title/nftables , abgerufen: 2024	31
nftables Vorlage Simple Ruleset	
https://wiki.nftables.org/wiki-nftables/index.php/Simple_ruleset_for_a_server , 2022	31
Wazuh Alert Archivierung	
https://documentation.wazuh.com/current/user-manual/wazuh-indexer/wazuh-indexer-indices.html#wazuh-archives-indices , abgerufen: 2024	32

12Anhang

12.1 Arbeitsjournal

Arbeitsjournal und Zeitplanung

Nachverfolgung des Arbeitsfortschritts

SOLL-Zeiten und Arbeitseinteilung

Bei 25-30h Aufwand pro ECTS ergibt sich für die Bachelor-Thesis mit 12 ECTS ein Aufwandsfenster von 300-360h.

Der grösste Teil des Arbeitsaufwandes soll sich auf 16 Semesterwochen verteilen. Mit 20h pro Woche kommen so 320h zustande.














Nach diesen 16 Semesterwochen und geplanten 320h wird noch Arbeit zur Vorbereitung und Durchführung der Verteidigung geleistet.

Die Hauptarbeitszeiten sind jeweils Dienstag, Mittwochnachmittag, sowie Samstagvormittag.

Während der Frühlingsferien in KW 15 sind keine Arbeitspakete einzuplanen.

Arbeitsumgebung

Zur Erarbeitung der Thesis wird ein Windows 10 Notebook verwendet. Es wurde eine Ordnerstruktur erstellt, welche die verschiedenen Komponenten der Arbeit übersichtlich ablegt, der Ordner wird mit dem Betreuer über Microsoft OneDrive geteilt.

Name	Status	Änderungsdatum	Typ
 00_Vorgaben	✓ R	22.02.2024 18:12	Dateiordner
 05_Informationsbeschaffung	✓ R	12.03.2024 11:08	Dateiordner
 06_Ressourcen	✓ R	07.05.2024 18:26	Dateiordner
 07_Bilder	✓ R	07.05.2024 18:44	Dateiordner
 09_Diagramme	✓ R	04.05.2024 17:23	Dateiordner
 10_Projektmanagement	↻ R	09.05.2024 07:51	Dateiordner
 11_Sitzungsprotokolle	✓ R	04.05.2024 10:19	Dateiordner
 80_Book-Eintrag	✓ R	20.02.2024 09:46	Dateiordner
 81_Film	✓ R	20.02.2024 08:36	Dateiordner
 82_Poster_und_Ausstellung	✓ R	20.02.2024 08:36	Dateiordner
 83_Techday_Präsentation	✓ R	07.05.2024 09:12	Dateiordner
 90_Verteidigung	✓ R	05.03.2024 09:01	Dateiordner
 Bachelor_Thesis_SIEM_Bericht.docx	↻ R	09.05.2024 07:50	Microsoft Word-D...

OneDrive ist die erste Backup-Ebene, zusätzlich wurde ein Git-Repository erstellt. Spätestens am Ende des Arbeitstages wird ein Commit erstellt und das Repository auf den GitLab-Server der BFH gepusht.

Zu guter Letzt wird der ganze Ordner jede Woche auf eine externe Festplatte kopiert.

Termine und Meilensteine

19.02.2024	Einführungsveranstaltung
20.02.2024	Kick-Off-Meeting (MS Teams)
27.02.2024	Projekt-Meeting (MS Teams)
04.03.2024	Deliverables / Ziele definiert
12.03.2024	Projekt-Meeting (MS Teams)
20.03.2024	Projekt Meeting Lab (MS Teams)
02.04.2024	Meeting mit Experte (Rolex Gebäude)
03.04.2024	Projekt Meeting (MS Teams)
16.04.2024	Projekt Meeting (MS Teams)
30.04.2024	Projekt Meeting (MS Teams)
21.05.2024	Projekt Meeting (MS Teams)
28.05.2024	Abgabe Poster
31.05.2024	Abgabe «Book»
13.06.2024	Abgabe Film
13.06.2024	Abgabe Schlussbericht
14.06.2024	Techday Präsentation / Ausstellung
26.06.2024	Verteidigung

SW 1

19.02.2024 – 18.02.2024

Wochenziele: Arbeits- und Zeitplanung erstellt
Dokumentenablage und Arbeitsumgebung verfügbar
Überblick zu SIEM gewinnen

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Montag	2h	<ul style="list-style-type: none">- Einführungsveranstaltung- Vorbereitung Kick-Off
Dienstag	10h	<ul style="list-style-type: none">- Kick-Off-Meeting- Erstellung Arbeits- und Dokumentenumgebung- Zeitplanung- Überblick SIEM gewinnen
Mittwoch	5h	<ul style="list-style-type: none">- Überblick SIEM gewinnen- Brainstorming Zieldefinition
Donnerstag	1h	<ul style="list-style-type: none">- Zeitplanung- Brainstorming Zieldefinition
Freitag	2h	<ul style="list-style-type: none">- Überblick SIEM gewinnen

IST-Wochentotal: 20h

SOLL-Gesamttotal: 20h

IST -Gesamttotal: 20h

SW 2

26.02.2024 – 03.03.2024

Wochenziele: Zieldefinition in Bericht aufnehmen
Kontaktaufnahme mit Experte
Beginn Kapitel zu «SIEM Allgemein»

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	5h	<ul style="list-style-type: none">- Projekt-Meeting- Überblick SIEM gewinnen
Mittwoch	10h	<ul style="list-style-type: none">- Kontaktaufnahme mit Experte- Zieldefinition in Bericht aufnehmen- Einleitung schreiben- Recherche SIEM
Samstag	5h	<ul style="list-style-type: none">- Beginn Kapitel «SIEM Allgemein»

IST-Wochentotal: 20h

SOLL-Gesamttotal: 40h

IST -Gesamttotal: 40h

Zielerreichung Vorwoche:

Alle Wochenziele der Vorwoche wurden erreicht.

SW 3

04.03.2024 – 10.03.2024

Wochenziele: Kapitel zu «SIEM Allgemein» abschliessen
Beginn Kapitel «Marktübersicht SIEM»
optional: Unterkapitel zu IDMEF erstellen

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Kapitel «SIEM Allgemein»- Diagramm «SIEM»
Mittwoch	5h	<ul style="list-style-type: none">- Kapitel «SIEM Allgemein» abschliessen- Unterkapitel «Aufbau eines SIEM» abschliessen- Expertentermin organisieren
Donnerstag	2h	<ul style="list-style-type: none">- Informationsbeschaffung «Marktübersicht»- Beginn Kapitel «Marktübersicht»
Samstag	3h	<ul style="list-style-type: none">- Vorbereitung Projekt-Meeting und Planung- Kapitel «Marktübersicht»

IST-Wochentotal: 20h

SOLL-Gesamttotal: 60h

IST -Gesamttotal: 60h

Zielerreichung Vorwoche:

Alle Wochenziele der Vorwoche wurden erreicht.

SW 4

11.03.2024 – 17.03.2024

Wochenziele: Kapitel «Marktübersicht SIEM» abschliessen
saubere Definition «SIEM» erstellen
optional: Produkte die nicht unter SIEM-Definition fallen auflisten
Termin Verteidigung planen

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Planung- Projekt-Meeting- Recherche SIEM-Markt- Tabelle «Marktübersicht SIEM»
Mittwoch	5h	<ul style="list-style-type: none">- Recherche SIM vs SEM vs SIEM- Definition SIEM- Recherche «SIEM-Kategorisierung»
Samstag	5h	<ul style="list-style-type: none">- Kapitel «SIEM-Kategorisierung» fertigstellen- Quellen nachführen

IST-Wochentotal: 20h

SOLL-Gesamttotal: 80h

IST -Gesamttotal: 80h

Zielerreichung Vorwoche:

Die Ziele der Vorwoche wurden mit Ausnahme des Unterkapitels zu IDMEF erreicht.
Dieses optionale Ziel kann zu einem späteren Zeitpunkt weiterverfolgt werden.

SW 5

18.03.2024 – 14.03.2024

Wochenziele: Termin Verteidigung planen
Ablauf «Requirements Engineering» definieren
Requirements an Lösung aufnehmen

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Administratives Book & Foto- Vorbereitung Requirements Engineering- Abkürzungsverzeichnis nachführen- Recherche SIEM-Funktionen
Mittwoch	6h	<ul style="list-style-type: none">- Meeting Anforderungen und Einführung Lab- Aufnahme der Anforderungen- Planung
Donnerstag	2h	<ul style="list-style-type: none">- Vorbereitung Kapitel «Requirements Engineering»- Beginn Kapitel «Requirements Engineering»
Freitag	2h	<ul style="list-style-type: none">- «Requirements Engineering» anhand Sitzungsnotizen

IST-Wochentotal: 20h

SOLL-Gesamttotal: 100h

IST -Gesamttotal: 100h

Zielerreichung Vorwoche:

Die beiden Ziele «Abschluss Marktübersicht» und «Definition SIEM», sowie das optionale Ziel «SIEM-Kategorisierung» wurden erreicht. Ein Terminvorschlag für die Verteidigung wurde gemacht, jedoch erhielt ich noch keine Antwort.

SW 6

25.03.2024 – 31.03.2024

Wochenziele: Anforderungen an SIEM in Bericht definieren
Evaluation SIEM
Mitteilung an Cyberlab-Team mit Systemanforderungen

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Anforderungen an SIEM definieren- Anforderungen an Umsetzung definieren- Evaluation vorbereiten
Mittwoch	5h	<ul style="list-style-type: none">- Evaluation SIEM (Bewertung)- Systemanforderungen an Cyberlab-Team- Variantenentscheid SIEM
Donnerstag	8h	<ul style="list-style-type: none">- Erweiterung Bericht Kapitel Requirements Engineering- Abschluss Requirements Engineering- Planung- IDMEF Format in Bericht erklären

IST-Wochentotal: 23h

SOLL-Gesamttotal: 120h

IST -Gesamttotal: 123h

Zielerreichung Vorwoche:

Die beiden Ziele «Ablauf Requirements Engineering» und «Anforderungen aufnehmen» konnten erreicht werden. Ein Termin für die Verteidigung steht noch nicht fest, dieses Ziel wird für nächste Woche zusammen mit dem Expertenmeeting eingeplant.

SW 7 + KW 15 (unterrichtsfreie Zeit)

01.04.2024 – 07.04.2024 (+ 08.04.2024 – 14.04.2024)

Wochenziele: Termin Verteidigung planen
Portrait-Foto und Expertentermin in Biel
Zugriff auf Cyberlab bekommen
Titel für Book bestimmen
Beginn Proof of Concept

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Portrait-Foto für Book-Eintrag- Expertenmeeting Rolex-Gebäude
Mittwoch	5h	<ul style="list-style-type: none">- Projekt-Meeting- Planung- Meeting Infrastruktur
Samstag	1h	<ul style="list-style-type: none">- Sitzungsprotokolle- Planung
Mittwoch KW 15	2h	<ul style="list-style-type: none">- Installation Wazuh Server- Organisation Installation Wazuh Agents

IST-Wochentotal: 18h

SOLL-Gesamttotal: 140h

IST -Gesamttotal: 141h

Zielerreichung Vorwoche:

Die Ziele der Vorwoche konnten alle erreicht werden. Das Requirements Engineering und die Evaluation kann in dieser Woche abschliessend besprochen werden, das Cyberlab-Team kennt meine Anforderungen. Ausserdem wurde der Eintrag zu IDMEF erstellt und damit neben den zwei Muss-Zielen M3 und M4 noch das Kann-Ziel K1 erledigt.

SW 8

15.04.2024 – 21.04.2024

Wochenziele: Wazuh-Oberfläche kennenlernen
Beginn Dokumentation PoC
Funktionsliste Wazuh schreiben

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Wazuh Oberfläche mit Agentendaten inspizieren- Projekt-Meeting- Inbetriebnahme VM «thesis-siem-client»
Mittwoch	5h	<ul style="list-style-type: none">- Funktionsliste Wazuh schreiben
Donnerstag	2h	<ul style="list-style-type: none">- Wazuh Wissensbeschaffung
Samstag	3h	<ul style="list-style-type: none">- Wazuh Wissensbeschaffung

IST-Wochentotal: 20h

SOLL-Gesamttotal: 160h

IST -Gesamttotal: 161h

Zielerreichung Vorwoche:

Die Ziele der Vorwoche wurden allesamt erreicht. Während der Unterrichtsfreien Zeit in KW 15, konnte der Wazuh Server installiert werden.

SW 9

22.04.2024 – 28.04.2024

Wochenziele: Eingabe Titeldaten «Book»
PoC «Systemumgebung» dokumentieren
PoC «Wazuh Architektur» dokumentieren
PoC «Installation» dokumentieren

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Vorbereitung PoC Dokumentation- Analyse Wazuh
Mittwoch	5h	<ul style="list-style-type: none">- PoC Dokumentation «Systemumgebung»- PoC Dokumentation «Installation»- Eingabe Titeldaten «Book»
Freitag	3h	<ul style="list-style-type: none">- Vorbereitung Dokumentation PoC «Zielüberprüfung»- PoC Dokumentation «Wazuh Architektur»
Samstag	3h	<ul style="list-style-type: none">- SSL Zertifikat CLAB für Wazuh installieren

IST-Wochentotal: 21h

SOLL-Gesamttotal: 180h

IST -Gesamttotal: 182h

Zielerreichung Vorwoche:

Die Ziele von letzter Woche konnte ich grundsätzlich erreichen, auch wenn ich im Bereich der PoC-Dokumentation noch nicht soviel Fortschritt gemacht habe, wie ich mir erhofft hatte.

SW 10

29.04.2024 – 05.05.2024

Wochenziele: PoC «Security Considerations» dokumentieren
PoC Konfiguration Host-Firewall
PoC Beginn Dokumentation «Zielabdeckung»

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Projekt-Meeting- PoC Dokumentation «Security Considerations»
Mittwoch	5h	<ul style="list-style-type: none">- PoC Konfiguration Host-Firewall- PoC Dokumentation «Security Considerations»
Samstag	6h	<ul style="list-style-type: none">- PoC Dokumentation Host Firewall- PoC Dokumentation verschlüsselte Kommunikation- PoC Kapitel «Security Considerations» fertigstellen

IST-Wochentotal: 21h

SOLL-Gesamttotal: 200h

IST -Gesamttotal: 203h

Zielerreichung Vorwoche:

Die Ziele der Vorwoche konnten erreicht werden. Zusätzlich konnte auch noch das SSL-Zertifikat für Wazuh installiert werden. Dabei bin ich auf Herausforderungen mit dem Zertifikat und Wazuh gestossen, welche ich durch die Verwendung eines Reverse-Proxys lösen konnte.

SW 11

06.05.2024 – 12.05.2024

Wochenziele: PoC Dokumentation «Zielabdeckung» fertigstellen
Beginn «Konzept produktiver Betrieb»

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Konfiguration E-Mail-Channel in Wazuh- Konfiguration E-Mail Alerts bei Security Event- PoC Dokumentation «Zielabdeckung»
Mittwoch	3h	<ul style="list-style-type: none">- Konzeptionierung «Überführung in produktiven Betrieb»
Donnerstag	4h	<ul style="list-style-type: none">- Vorbereitung Plakat- Nachführen Literaturverzeichnis- Dokumentation «E-Mail-Benachrichtigungen»
Samstag	6h	<ul style="list-style-type: none">- Dokumentation «Überführung in produktiven Betrieb»- Abschluss PoC Dokumentation

IST-Wochentotal: 23h

SOLL-Gesamttotal: 220h

IST -Gesamttotal: 226h

Zielerreichung Vorwoche:

In der Vorwoche konnte ich wie geplant das Kapitel um die «Security Considerations» abschliessen, jedoch noch nicht mit der Dokumentation der Zielabdeckung beginnen. Dies ist für diese Woche geplant.

SW 12

13.05.2024 – 19.05.2024

Wochenziele: Dokumentation «Schlussfolgerung/Fazit»
Dokumentation «Management Summary»
Beginn «Poster»
Beginn «Book»

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	7h	<ul style="list-style-type: none">- Zielüberprüfung Projektziele- Beginn Dokumentation «Schlussfolgerung/Fazit»
Mittwoch	5h	<ul style="list-style-type: none">- Planung Abgaben und Termine- Konzeptionierung Poster und Book
Donnerstag	3h	<ul style="list-style-type: none">- Dokumentation «Schlussfolgerung/Fazit»
Samstag	4h	<ul style="list-style-type: none">- Diagramme verbessern- Beginn Book-Eintrag schreiben

IST-Wochentotal: 19h

SOLL-Gesamttotal: 240h

IST -Gesamttotal: 245h

Zielerreichung Vorwoche:

Die Ziele der Vorwoche konnte ich erreichen und sogar übertreffen. Die Dokumentation der Zielabdeckung wurde fertiggestellt, das Konzept zur Überführung in den produktiven Betrieb ebenfalls.

SW 13

20.05.2024 – 26.05.2024

Wochenziele: Book-Eintrag abschliessen
Poster abschliessen
Management Summary schreiben
Diagramme «Einführung SIEM» überarbeiten
Konzept «Film» erstellen

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Montag	4h	<ul style="list-style-type: none">- Book-Eintrag fertigstellen- Poster erstellen- Diagramme «Einführung SIEM» überarbeiten
Dienstag	8h	<ul style="list-style-type: none">- Beginn Konzeptionierung Film- Projekt-Meeting
Mittwoch	5h	<ul style="list-style-type: none">- Book-Eintrag und Poster abgeben- Management Summary / Abstract einfügen- Film Konzept
Freitag	1h	<ul style="list-style-type: none">- Test Cyberlab-Zugriff aus BFH-WLAN- Film Konzept
Samstag	2h	<ul style="list-style-type: none">- Korrekturlesen Dokumentation

IST-Wochentotal: 20h

SOLL-Gesamttotal: 260h

IST -Gesamttotal: 265h

Zielerreichung Vorwoche:

Ich konnte das Fazit schreiben und mit dem Book-Eintrag beginnen, die Management-Summary habe ich jedoch noch nicht begonnen. Hierfür erhoffe ich mir einen Nutzen aus Book und Poster ziehen zu können.

SW 14

27.05.2024 – 02.06.2024

Wochenziele: Film erstellen
Beginn Präsentation Techday
Bericht verbessern

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Film Screen Recordings erstellen- Film Tonaufnahmen erstellen- Film schneiden- BFH Netzwerk Cyberlab-Zugang Debugging
Mittwoch	5h	<ul style="list-style-type: none">- Film abgeben- Book-Eintrag an Sekretariat weiterleiten- Beginn Präsentation Techday
Freitag	1h	<ul style="list-style-type: none">- Fehlersuche Cyberlab Zugang BFH-Netzwerk
Samstag	5h	<ul style="list-style-type: none">- Korrekturlesen Bericht- Glossar und Verzeichnisse pflegen- Anhänge einfügen

IST-Wochentotal: 21h

SOLL-Gesamttotal: 280h

IST -Gesamttotal: 286h

Zielerreichung Vorwoche:

Das Poster konnte letzte Woche abgeschlossen und abgegeben werden, der Book-Eintrag wurde zur Freigabe an Herrn Wenger weitergeleitet. Auch die Anpassungen der Diagramme im Bericht und die erste Konzeptionierung des Films konnte gemacht werden. Die Management-Summary wurde ebenfalls erstellt, somit wurden die Ziele der Vorwoche erreicht.

SW 15

03.06.2024 – 09.06.2024

Wochenziele: Demo Präsentation Techday erstellen
Präsentation Techday erstellen
Bericht finalisieren

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	- Demo Präsentation erstellen - Präsentation Techday erstellen
Mittwoch	5h	- Präsentation Techday erstellen
Samstag	5h	- Präsentation Techday erstellen
Sonntag	2h	- Präsentation Techday üben - Bericht verbessern

IST-Wochentotal: 22h

SOLL-Gesamttotal: 300h

IST -Gesamttotal: 308h

Zielerreichung Vorwoche:

Letzte Woche konnte der Film erstellt und abgegeben werden, damit wurde das Hauptziel erreicht. Auch der Bericht konnte verbessert werden und die ersten Schritte der Präsentation erstellt, die Ziele der Vorwoche wurden damit erreicht.

SW 16

10.06.2024 – 16.06.2024

Wochenziele: Bericht abgeben
Präsentation finalisieren und halten

Hinweis: *Kursiv geschriebene Zeitangaben sind Schätzungen, welche zum Zeitpunkt der Dokumenterstellung noch in der Zukunft liegen.*

SOLL: 20h

Arbeitszeiten:

Tag	Zeitaufwand	Arbeiten
Dienstag	10h	<ul style="list-style-type: none">- Techday-Präsentation vorbereiten- Techday-Präsentation üben- Bericht finalisieren- Berichtsabgabe
Mittwoch	5h	<ul style="list-style-type: none">- <i>Bericht drucken</i>- <i>Techday-Präsentation üben</i>
Freitag	5h	<ul style="list-style-type: none">- <i>Techday-Präsentation halten</i>- <i>Ausstellungsstand Techday betreuen</i>

IST-Wochentotal: 20h

SOLL-Gesamttotal: 320h

IST -Gesamttotal: 328h

Zielerreichung Vorwoche:

Die Demo für die Präsentation konnte erstellt werden und der Bericht ist inhaltlich fertig. Es fehlt noch der Anhang und die Unterschrift auf der Selbständigkeitserklärung. Auch die Techday-Präsentation konnte fast fertiggestellt werden, einige Details werden noch angepasst.

Nach Ende der regulären Unterrichtszeit wird die Verteidigungspräsentation vorbereitet und durchgeführt.

Total bis Verteidigung 26.06.2024 ≈ 360h

12.2 Sitzungsprotokolle

Sitzungsprotokoll

Kick-Off-Meeting, 20.02.2024

Anwesend: Hansjürg Wenger
Sven Trachsel

Traktanden / Beschlüsse:

- Datenaustausch via Freigabe von OneDrive-Ordner
 - o Sitzungsprotokolle werden nur auf OneDrive abgelegt (kein Verteiler)
- Bericht Deutsch in Word (Vorlage Bachelor-Thesis BFH)
- Meetings 2-wöchentlich, Ausnahme SW2
- Arbeitszeiterfassung in Form Arbeitsjournal mit Inhalt
 - o Wochentag
 - o Arbeitszeit
 - o Aufgaben
 - o SOLL/IST Totalzeiten
- Planung mit 20h pro Woche bei 15 Wochen
- Sobald Experte bekannt, Kontakt aufnehmen
- Erstes Kapitel Thesis-Dokument: Überblick und Fähigkeiten SIEM
- Fragen zwischen Meetings per E-Mail an Hansjürg Wenger

bis zum nächsten Meeting zu erledigen:

- Zeitplanung mit Deadlines
- Vorgehen definieren
- ersten Überblick SIEM gewinnen
- Vorbereitung, um Deliverables zu definieren

nächstes Meeting: 27.02.2024

Sitzungsprotokoll

Meeting, 27.02.2024

Anwesend: Hansjürg Wenger
Sven Trachsel

Traktanden / Beschlüsse:

- Überprüfung Zeitplan (GANTT-Diagramm) und Arbeitsjournal
 - o Format und Inhalt ok
- Muss-Projektziele angeschaut
 - o - (Der Bericht enthält eine) Einführung in SIEM in Doku
 - o - Marktübersicht SIEM-Lösungen erstellen (wie vollständig?)
 - o - Requirements an SIEM-Lösung für Laborumgebung aufnehmen
 - o - Evaluation der SIEM-Lösung für Laborumgebung
 - o - PoC der gewählten SIEM-Lösung für Laborumgebung (mit Evaluation der Funktion)
 - o - Vorschlag für Überführung in produktiven Betrieb
- Kann-Projektziele angeschaut
 - o - IDMEF Message Format erklärt
 - o - PoC Lösung in Produktionsreife Lösung umbauen
 - o - Produkte die sich als SIEM bezeichnen, aber keines sind (Abgrenzung)
- Testing auf Labor-Setup n049 von Project 2
- Bis Mitte März wird neues Laborsetup zur Verfügung gestellt für PoC

bis zum nächsten Meeting zu erledigen:

- Kontaktaufnahme mit Experte
 - o Woche für Verteidigung abklären
- Projektziele in Bericht aufnehmen

nächstes Meeting: 12.03.2024

Sitzungsprotokoll

Meeting, 12.03.2024

Anwesend: Hansjürg Wenger
Sven Trachsel

Traktanden / Beschlüsse:

- Fortschritt gezeigt, im Zeitplan
- Meeting nötig, um Anforderungen an SIEM aufzunehmen
 - o Am 20.03. 14:30 bis 15:30
 - o Donatello Gallucci wird auch anwesend sein
- Umgebung für Umsetzung wird an Meeting nächste Woche besprochen
- Verteidigung ev. am 26.06.

bis zum nächsten Meeting zu erledigen:

- Fragenkatalog für Meeting von 20.03. falls vorhanden bis 19.03. an Herrn Wenger senden
- Termin für Verteidigung mit Experte suchen

nächstes Meeting: 20.03.2024

Sitzungsprotokoll

Meeting, 20.03.2024

Anwesend: Hansjürg Wenger
Kevin Schrag
Donatello Gallucci
Sven Trachsel

Traktanden / Beschlüsse:

- Aufnahme von Informationen zu Anforderungen:
 - o Anwender
 - o Umfeld
 - o Systemnutzen
 - o Weitere Anforderungen
- Details in Bericht, wichtige Punkte hier aufgeführt
 - o Muss nachvollziehbar und reproduzierbar sein
 - o Hilfestellung / Erstellung eventueller Ansible-Playbooks anhand meiner Konfiguration durch Donatello Gallucci
 - o Relevant für BA-Thesis ist Playground-Teil des Lab
- Kontakt Lab für Fragen: Kevin Schrag (kevin.schrag@bfh.ch), CC an Donatello Gallucci (donatello.gallucci@bfh.ch)

bis zum nächsten Meeting zu erledigen:

- Info an Kevin Schrag, wenn klar ist welche Ressourcen benötigt werden
- Wireguard Public Key an Kevin Schrag

nächstes Meeting: 03.04.2024

Sitzungsprotokoll

Expertenmeeting, 02.04.2024

Anwesend: Thomas Jäggi
Sven Trachsel

Traktanden / Beschlüsse:

- Verteidigungstermin Mittwoch 26.06. 14:00 bis 16:00 Uhr ist ok
- Berichtsabgabe per E-Mail
- Grafiken verwenden in Bericht
- SIEM bietet Möglichkeiten für eine anschauliche Demo
- Für Verteidigung: Wo könnte Wazuh helfen, was ist der Nutzen (z.B. KMU)?

zu erledigen:

- Ort und definitive Uhrzeit der Verteidigung mitteilen

Sitzungsprotokoll

Meeting, 03.04.2024

Anwesend: Hansjürg Wenger
Sven Trachsel

Traktanden / Beschlüsse:

- Arbeitstitel «SIEM für Laborumgebungen» ist ok
- Termin für Verteidigung gesetzt auf Mi. 26.06. 14:00 bis 16:00 Uhr
 - o Ort: SIPBB, Raum folgt durch wgh1
- Variantenentscheid ist gefällt, gewählte Lösung ist Wazuh

bis zum nächsten Meeting zu erledigen:

- wgh1: bei K. Schrag nachfragen, wann Umgebung bereit ist

nächstes Meeting: 16.04.2024

Sitzungsprotokoll

Meeting Infrastruktur, 03.04.2024

Anwesend: Kevin Schrag
Sven Trachsel

Traktanden / Beschlüsse:

- Zugang zu Netzwerk mit Wireguard erhalten und getestet
- Zugang zu VM «thesis-siem» mit SSH-Key erhalten und getestet
 - o IP-Adresse: 192.168.230.160
 - o inklusive Passwort für sudo
- vorhandene Infrastruktur erklärt
- Server bei IP 192.168.230.150 nicht anfassen, für Project 1 Arbeit in Verwendung
- Konfigurationsrichtlinien besprochen:
 - o Sane-defaults für Security-Richtlinien
 - nur TLS (am besten 1.3)
 - wäre gut wenn nftables enthalten
 - eventuell Zero-Trust
 - o Drop-In Mechanismen für Konfigurationen verwenden
- Zertifikat für Hostname und IP von interner CA erhalten
 - o Root-Zertifikat auch erhalten für eigenen Browser
- Zentraler journald-Server vorhanden, eventuell können Logs von dort geholt werden

Sitzungsprotokoll

Meeting, 16.04.2024

Anwesend: Hansjürg Wenger
Sven Trachsel

Traktanden / Beschlüsse:

- Aktuellen Stand gezeigt, Wazuh Server und 6 Agenten stehen
- E-Mail Weiterleitung bei nslab SMTP-Server eingerichtet, für Alerting
 - o Absender: wazuh@nslab.ch
 - o Weiterleitung an: sven.trachsel@students.bfh.ch
- Abschnitt «Featureliste» in Evaluationsteil einfügen, versprochene Features von Wazuh aufzeigen
 - o In PoC verwendete Features beschreiben

bis zum nächsten Meeting zu erledigen:

- Baldmöglichst Kontakt mit Kevin Schrag aufnehmen für weitere VM, damit Tests mit eigenen Agenten-Installationen gemacht werden können

nächstes Meeting: 30.04.2024

Sitzungsprotokoll

Meeting, 30.04.2024

Anwesend: Hansjürg Wenger
Sven Trachsel

Traktanden / Beschlüsse:

- Arbeit ist auf gutem Weg
- für Verteidigung ev. Interpretation von Werten aus SIEM
- Hj. Wenger über Pfinsten nicht erreichbar
- K. Schrag arbeitet jeweils bis Mittwochs, falls für PoC noch Kontakt nötig
 - o Bei Konfiguration nftables K. Schrag kontaktieren wenn ich mich aussperre

bis zum nächsten Meeting zu erledigen:

- weiter gemäss Projektplanung

nächstes Meeting: 21.05.2024

Sitzungsprotokoll

Meeting, 21.05.2024

Anwesend: Hansjürg Wenger
Sven Trachsel

Traktanden / Beschlüsse:

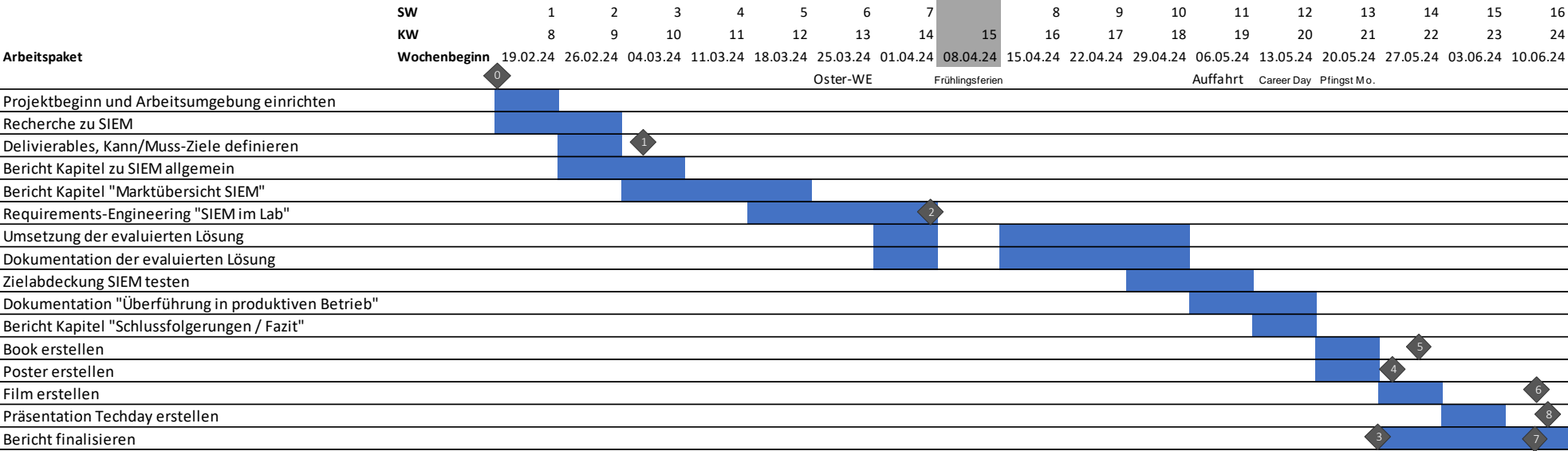
- private IP-Adressen aus Labornetz dürfen im Film gezeigt werden
- Book und Poster sehen inhaltlich ok aus
- kein Meeting mehr bis zum Finaltag

bis zum nächsten Meeting zu erledigen:

- Arbeit fertigstellen und abgeben

nächstes Meeting: Finaltag / Techday

12.3 GANTT-Diagramm



Meilensteine		
Nr	Meilenstein	Datum
0	Projektbeginn	19.02.2024
1	Deliverables / Ziele definiert	05.03.2024
2	Variantenentscheid SIEM	07.04.2024
3	Content-Freeze Bericht	26.05.2024
4	Abgabe Poster	28.05.2024
5	Abgabe "Book"	31.05.2024
6	Abgabe Film	13.06.2024
7	Abgabe Schlussbericht	13.06.2024
8	Techday Präsentation / Ausstellung	14.06.2024
9	Verteidigung	26.06.2024

12.4 Wazuh Firewall Konfiguration

Datei «/etc/nftables.conf» von Server «thesis-siem».

Quelle Vorlage: https://wiki.nftables.org/wiki-nftables/index.php/Simple_ruleset_for_a_server

```
#!/usr/sbin/nft -f

flush ruleset

table inet firewall {

    chain inbound_ipv4 {
        # accepting ping (icmp-echo-request) for diagnostic purposes.
        # However, it also lets probes discover this host is alive.
        # This sample accepts them within a certain rate limit:

        icmp type echo-request limit rate 5/second accept
    }

    chain inbound_ipv6 {
        # accept neighbour discovery otherwise connectivity breaks
        #
        icmpv6 type { nd-neighbor-solicit, nd-router-advert, nd-neighbor-advert
    } accept

        # accepting ping (icmpv6-echo-request) for diagnostic purposes.
        # However, it also lets probes discover this host is alive.
        # This sample accepts them within a certain rate limit:

        icmpv6 type echo-request limit rate 5/second accept
    }

    chain inbound {

        # By default, drop all traffic unless it meets a filter
        # criteria specified by the rules that follow below.
        type filter hook input priority 0; policy drop;

        # Allow traffic from established and related packets, drop invalid
        ct state vmap { established : accept, related : accept, invalid : drop }

        # Allow loopback traffic.
        iifname lo accept
    }
}
```

```

# Jump to chain according to layer 3 protocol using a verdict map
meta protocol vmap { ip : jump inbound_ipv4, ip6 : jump inbound_ipv6 }

# Allow SSH on port TCP/22 and allow HTTP(S) TCP/80 and TCP/443
# for IPv4 and IPv6.
tcp dport { 22, 80, 443} accept

# allow wazuh server traffic
tcp dport {1514, 1515, 1516, 55000} accept

# allow wazuh indexer traffic
tcp dport 9200 accept
tcp dport 9300-9400 accept

# log prefix "[nftables] Inbound Denied: " counter drop
}

chain forward {
    # Drop everything (assumes this device is not a router)
    type filter hook forward priority 0; policy drop;
}

# no need to define output chain, default policy is accept if undefined.
}

```

12.5 NGINX Revere Proxy Konfiguration

Datei «/etc/nginx/sites-available/wazuh-dashboard-proxy» von Server «thesis-siem».

Quelle Vorlage: SSL-Konfiguration nginx mit Let's Encrypt,

<https://www.nginx.com/blog/using-free-ssl-tls-certificates-from-lets-encrypt-with-nginx/>

```
server {

    server_name thesis-siem.clab.playground thesis-siem 192.168.230.160;

    location / {
        proxy_pass https://192.168.230.160:9101;
        proxy_set_header Host $host;
    }

    listen 443 ssl;
    ssl_certificate /etc/ssl-int/siem.crt;
    ssl_certificate_key /etc/ssl-int/siem.key;

}

server {

    if ($host = 192.168.230.160) {
        return 301 https://$host$request_uri;
    }

    listen 80 default_server;

    server_name 192.168.230.160;
    return 404;

}
```

13 Selbständigkeitserklärung

Ich bestätige, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der im Literaturverzeichnis angegebenen Quellen und Hilfsmittel angefertigt habe. Sämtliche Textstellen, die nicht von mir stammen, sind als Zitate gekennzeichnet und mit dem genauen Hinweis auf ihre Herkunft versehen.

Ort, Datum:

Oberdiessbach, 11.06.2024

Unterschrift:

A handwritten signature in black ink, reading "S. Trachsel". The signature is written in a cursive style with a large, stylized 'S' and a trailing flourish.



Erklärung der Diplomandinnen und Diplomanden *Déclaration des diplômant-e-s*

Selbständige Arbeit / *Travail autonome*

Ich bestätige mit meiner Unterschrift, dass ich meine vorliegende Bachelor-Thesis selbständig durchgeführt habe. Alle Informationsquellen (Fachliteratur, Besprechungen mit Fachleuten, usw.) und anderen Hilfsmittel, die wesentlich zu meiner Arbeit beigetragen haben, sind in meinem Arbeitsbericht im Anhang vollständig aufgeführt. Sämtliche Inhalte, die nicht von mir stammen, sind mit dem genauen Hinweis auf ihre Quelle gekennzeichnet.

Par ma signature, je confirme avoir effectué ma présente thèse de bachelor de manière autonome. Toutes les sources d'information (littérature spécialisée, discussions avec spécialistes etc.) et autres ressources qui m'ont fortement aidé-e dans mon travail sont intégralement mentionnées dans l'annexe de ma thèse. Tous les contenus non rédigés par mes soins sont dûment référencés avec indication précise de leur provenance.

Name/*Nom*, Vorname/*Prénom*

Sven Trachsel

Datum/*Date*

11.06.2024

Unterschrift/*Signature*

S. Trachsel

Dieses Formular ist dem Bericht zur Bachelor-Thesis beizulegen.
Ce formulaire doit être joint au rapport de la thèse de bachelor.