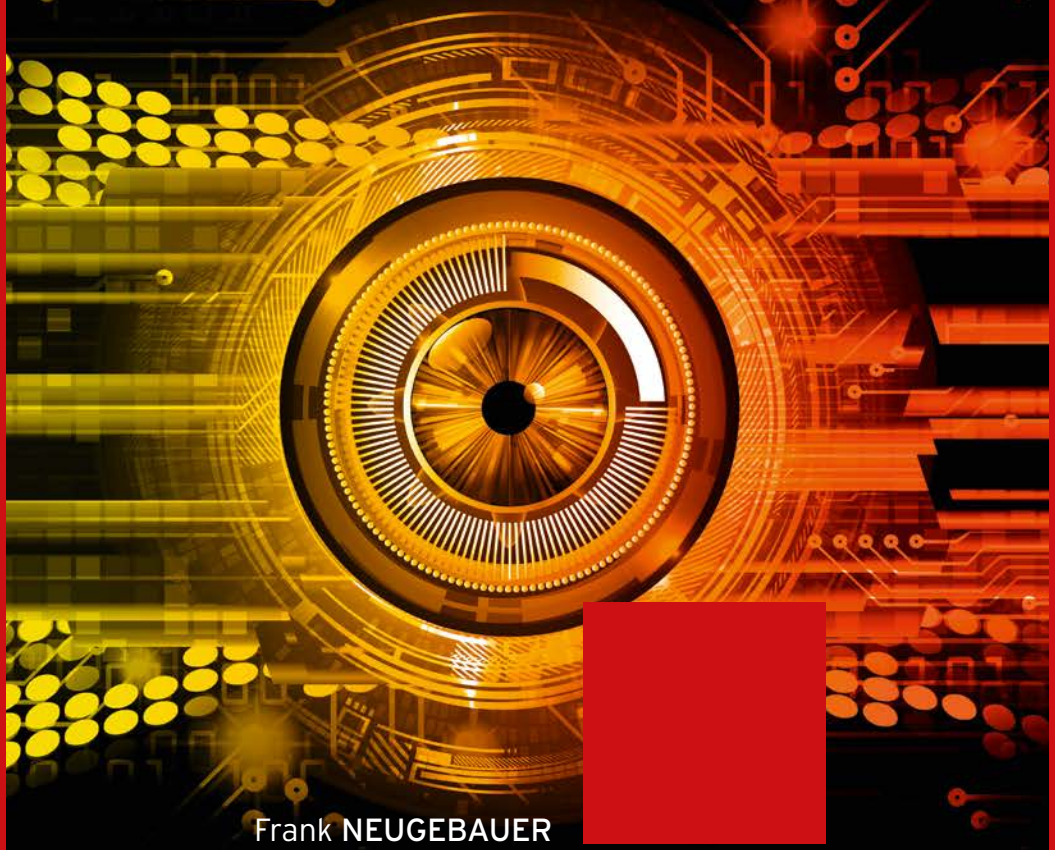

Frank NEUGEBAUER

CYBERSICHERHEIT MIT WAZUH

Bedrohungen mit Open-Source-Software erkennen, analysieren und abwehren

HANSER

Neugebauer
Cybersicherheit mit Wazuh

Bleiben Sie auf dem Laufenden!

Der Hanser Computerbuch-Newsletter informiert Sie regelmäßig über neue Bücher und Termine aus den verschiedenen Bereichen der IT. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter

www.hanser-fachbuch.de/newsletter

Frank Neugebauer

Cybersicherheit mit Wazuh

Bedrohungen mit Open-Source-Software erkennen, analysieren und abwehren

HANSER

Der Autor: Frank Neugebauer
https://wazuh.frankneugebauer.eu

Print-ISBN: 978-3-446-48503-7
E-Book-ISBN: 978-3-446-48510-5
E-Pub-ISBN: 978-3-446-48566-2

Die allgemein verwendeten Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Alle in diesem Werk enthaltenen Informationen, Verfahren und Darstellungen wurden zum Zeitpunkt der Veröffentlichung nach bestem Wissen zusammengestellt. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Werk enthaltenen Informationen für Autor:innen, Herausgeber:innen und Verlag mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor:innen, Herausgeber:innen und Verlag übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Weise aus der Benutzung dieser Informationen – oder Teilen davon – entsteht. Ebenso wenig übernehmen Autor:innen, Herausgeber:innen und Verlag die Gewähr dafür, dass die beschriebenen Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt also auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benützt werden dürften.

Die endgültige Entscheidung über die Eignung der Informationen für die vorgesehene Verwendung in einer bestimmten Anwendung liegt in der alleinigen Verantwortung des Nutzers.

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://dnb.d-nb.de abrufbar.

Dieses Werk ist urheberrechtlich geschützt.
Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Werkes, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Einwilligung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder einem anderen Verfahren), auch nicht für Zwecke der Unterrichtgestaltung – mit Ausnahme der in den §§ 53, 54 UrhG genannten Sonderfälle –, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.
Wir behalten uns auch eine Nutzung des Werks für Zwecke des Text und Data Mining nach § 44b UrhG ausdrücklich vor.

© 2025 Carl Hanser Verlag GmbH & Co. KG, München
Vilshofener Straße 10 | 81679 München | info@hanser.de
www.hanser-fachbuch.de
Lektorat: Sylvia Hasselbach, Kristin Rothe
Herstellung: Gina Lada
Copy editing: Walter Saumweber, Ratingen
Coverkonzept: Marc Müller-Bremer, www.rebranding.de, München
Covergestaltung: Thomas West
Titelmotiv: © shutterstock.com/Titima Ongkantong
Satz: Eberl & Koesel Studio, Kempten
Druck: Elanders Waiblingen GmbH, Waiblingen
Printed in Germany

Inhalt

Geleitwort

Liebe Leserschaft,

mit großer Freude dürfen wir Ihnen dieses Buch über die Sicherheitsplattform Wazuh vorstellen. In Zeiten, in denen IT-Sicherheit komplexer und anspruchsvoller wird, bietet Wazuh eine beeindruckende Antwort auf viele aktuelle Herausforderungen – flexibel, leistungsstark und für verschiedenste Infrastrukturen geeignet.

Wir hatten das Privileg, Wazuh in unterschiedlichsten, auch international tätigen Unternehmen produktiv einzusetzen und konnten dabei aus erster Hand erfahren, wie vielseitig und robust diese Plattform in der Praxis funktioniert. Ob agentenloser Betrieb in Cloud-Umgebungen wie AWS oder die Integration in homo- und heterogene Netzwerklandschaften – Wazuh zeigt seine Stärken in verschiedensten Szenarien und unterstützt Organisationen dabei, Transparenz, Sicherheit und Compliance nachhaltig zu verbessern.

Gerade im Bereich Open Source zeigt sich die besondere Stärke: eine aktive Community, stetige Weiterentwicklung und die Möglichkeit, Lösungen flexibel an eigene Anforderungen anzupassen. Natürlich bringt diese Offenheit auch gewisse Herausforderungen mit sich. So können etwa Breaking Changes in Minor Updates den Einsatz von automatisierten Update-Mechanismen – etwa mit Ansible – erschweren. Solche Eigenheiten verlangen eine bewusste Planung und ein genaues Verständnis der eingesetzten Versionen, bevor Updates eingespielt werden; dieses Buch nimmt Sie dabei an die Hand.

Besonders hervorzuheben ist, dass die in diesem Buch dargestellten Use-Cases weit über die üblichen Beispiele und Standardanleitungen hinausgehen, die man im Internet findet.

Dieses Buch soll Ihnen helfen, Wazuh besser zu verstehen, seine Potenziale gezielt auszuschöpfen und pragmatische Wege für den erfolgreichen Einsatz in Ihrer Umge-

bung zu finden. Es ist eine Einladung, das volle Potenzial von Open-Source-Sicherheit zu entdecken – fundiert, nachvollziehbar und praxisnah.

Wir wünschen Ihnen eine spannende Lektüre und viele wertvolle Erkenntnisse auf Ihrem Weg mit Wazuh!

Beste Grüße

Michael Münz

https://www.max-it.de

m.a.x. Informationstechnologie AG

Landshuter Allee 12 – 14

D-80637 München

Vorwort

In der sich permanent weiterentwickelnden Welt der Cybersicherheit sind Unternehmen und Privatpersonen ständig auf der Suche nach effizienten und erschwinglichen Lösungen, um ihre digitalen Werte zu schützen. In diesem Zusammenhang bin ich auf ein bemerkenswert leistungsfähiges und dennoch kostenloses Tool gestoßen: Wazuh.

Meine Reise mit Wazuh begann, als ich auf ein faszinierendes YouTube-Video von John Hammond [1] stieß. In diesem Video stellte Hammond Wazuh als kostenlose Open-Source-Sicherheitsplattform vor, die SIEM- und XDR-Funktionen kombiniert. Seine Begeisterung für die Vielseitigkeit und Leistungsfähigkeit von Wazuh war ansteckend und weckte mein Interesse, tiefer in die Materie einzutauchen.

Das Video von Hammond war nur der Anfang. In der Folge entdeckte ich viele weitere Beiträge von Cybersicherheitsexperten und Bloggern, die alle die herausragenden Funktionen und den kostenlosen Ansatz von Wazuh hervorhoben. Diese kollektive Anerkennung bestärkte mich in meiner Überzeugung, dass Wazuh ein Tool ist, das es wert ist, näher betrachtet zu werden.

Die Popularität von Wazuh hat in den vergangenen Jahren beeindruckende Ausmaße angenommen. Derzeit sind auf Github [2] 163 Personen registriert, die aktiv am Projekt beteiligt sind. Noch bemerkenswerter ist die Tatsache, dass es laut der Wazuh-Webseite [3] die weltweit am häufigsten genutzte Open-Source-Sicherheitslösung ist. Die Plattform schützt über 15 Millionen Endpunkte, hat über 100 000 Unternehmenskunden und verzeichnet mehr als 30 Millionen Downloads pro Jahr.

Die breite Akzeptanz von Wazuh in verschiedenen Branchen unterstreicht seine Vielseitigkeit und Effizienz. Vom E-Commerce-Sektor, wo es zur Überwachung verdächtiger Transaktionen eingesetzt wird, bis zum Gesundheitswesen, wo es zur Einhaltung strenger Datenschutzbestimmungen beiträgt, hat sich Wazuh als unverzichtbares Werkzeug in der modernen Cybersicherheitslandschaft etabliert.

Wazuh wird bereits in 33 Ländern weltweit eingesetzt. Die deutlich stärkste Verbreitung ist in den USA zu verzeichnen, wo mindestens 126 Unternehmen [4] Wazuh einsetzen. In Deutschland nutzen nach den vorliegenden Daten mindestens 11 Unternehmen [5] Wazuh, darunter Unternehmen aus unterschiedlichen Branchen wie IT-Dienstleistungen, IT-Sicherheit und Telekommunikation. Bemerkenswert ist, dass sich unter den deutschen Nutzern auch ein großes Telekommunikationsunternehmen befindet. Derzeit ist Wazuh in Europa noch nicht sehr verbreitet, es ist aber von einem vielversprechenden Expansionspotenzial im europäischen Cybersicherheitsmarkt auszugehen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem Projekt „Codeanalyse von Open Source Software“ (CAOS) [6] herausgestellt, dass Open Source Software mindestens genauso sicher ist wie proprietäre Software. Durch die Offenlegung des Quellcodes können Schwachstellen schneller erkannt und behoben werden, was das Vertrauen in diese Lösungen stärkt.

Wazuh hat auch Einzug in die akademische Welt gehalten. So wurde es an der Berner Fachhochschule auf einem Server installiert und in verschiedenen Projekten eingesetzt, um den Studierenden praktische Erfahrungen im Bereich der IT-Sicherheit zu vermitteln. Weitere akademische Arbeiten beschäftigen sich ebenfalls mit diesem Thema.

Trotz seiner Leistungsfähigkeit und Kostenfreiheit ist es wichtig zu betonen, dass die effektive Nutzung von Wazuh persönliches Engagement und Lernbereitschaft erfordert. Die Software mag kostenlos sein, aber ihre optimale Implementierung und Nutzung erfordern Zeit, Geduld und den Willen, sich ständig weiterzubilden. Die Komplexität der heutigen Sicherheitsherausforderungen spiegelt sich in der Vielfalt der Funktionen von Wazuh wider, und es liegt an uns als Benutzern, das volle Potenzial dieses leistungsstarken Tools auszuschöpfen.

In diesem Buch möchte ich Sie auf eine Reise durch die Welt von Wazuh mitnehmen. Gemeinsam werden wir die Grundlagen erforschen, fortgeschrittene Techniken erlernen und praktische Anwendungsfälle untersuchen. Mein Ziel ist es, Ihnen das Wissen und die Werkzeuge an die Hand zu geben, damit Sie Wazuh effektiv in Ihrer eigenen Cybersicherheitsstrategie einsetzen können.

Aber ich möchte Sie von Anfang an darauf vorbereiten: Der Einstieg in dieses komplexe Thema ist nicht immer einfach. Die Welt der Cybersicherheit ist generell anspruchsvoll, und Wazuh als vielseitige Open-Source-Plattform besitzt eine steile Lernkurve. Rückschläge sind vorprogrammiert – Sie werden auf Fehler stoßen, an Konfigurationshürden scheitern und an manchen Stellen vielleicht das Gefühl haben, nicht weiterzukommen. Keine Sorge, das ist vollkommen normal.

Es kann frustrierend sein, wenn etwas nicht auf Anhieb funktioniert oder unerwartete Probleme auftauchen. Vielleicht gibt es sogar Momente, in denen man aufgeben möchte. Doch genau darin liegt die Herausforderung und zugleich die Chance: Wer durchhält, aus Fehlern lernt und sich nicht entmutigen lässt, wird am Ende nicht nur

Wazuh meistern, sondern auch ein tieferes Verständnis für Cybersicherheit insgesamt entwickeln.

Die IT-Sicherheitslandschaft entwickelt sich stetig weiter – und mit ihr auch Wazuh. Dieses Buch basiert auf dem aktuellen Stand der Software zum Zeitpunkt seiner Veröffentlichung (Version 4.11). Es ist selbstverständlich, dass künftige Versionen neue Funktionen einführen oder bestehende Konzepte anpassen werden. Gerade im produktiven Umfeld sollten Aktualisierungen jedoch stets sorgfältig geprüft und nicht unüberlegt übernommen werden.

Um Leserinnen und Leser über relevante Änderungen und Ergänzungen auf dem Laufenden zu halten, stellen wir aktuelle Hinweise und Ergänzungen auf der Website zum Buch [7] bereit. Bitte informieren Sie sich dort regelmäßig, um Ihr Wissen auf dem neuesten Stand zu halten.

Ich lade Sie hiermit ein, diese Reise mit mir zu wagen – mit Geduld, mit Neugier und mit der Bereitschaft, aus Hindernissen zu lernen. Denn am Ende wird es sich lohnen.

[1] John Hammond, Vorstellung Wazuh – *https://www.youtube.com/watch?v=i68atPbB8uQ*

[2] Wazuh GitHub – *https://github.com/wazuh*

[3] Wazuh über die Entwickler – *https://wazuh.com/about-us/*

[4] Unternehmen in den USA – *https://theirstack.com/de/technology/wazuh/us*

[5] Unternehmen in Deutschland – *https://theirstack.com/de/technology/wazuh/de*

[6] BSI und Open Source – *https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/Projekt_P486/projekt_P486_node.html*

[7] Website zum Buch „Cybersicherheit mit Wazuh“ – *https://wazuh.frankneugebauer.eu*

1 Über dieses Buch

1.1 Orientierung und Motivation

Willkommen bei „Cybersicherheit mit Wazuh“ – Ihrem Einstieg in die Welt der modernen IT-Sicherheit. In einer Zeit, in der Cyberbedrohungen allgegenwärtig sind und Angriffe immer raffinierter werden, ist es entscheidend, nicht nur reaktiv zu handeln, sondern proaktiv zu überwachen und zu schützen. Genau hier setzt Wazuh an. Die Open-Source-Sicherheitsplattform ermöglicht es Unternehmen und Privatpersonen, Bedrohungen zu erkennen, auf Sicherheitsvorfälle zu reagieren und Systeme kontinuierlich zu überwachen – und das alles in einer flexiblen, skalierbaren und kostenlosen Lösung.

Warum ist es also so wichtig, sich mit Wazuh zu beschäftigen? Die Antwort liegt in der sich ständig verändernden Bedrohungslandschaft. Angreifer entwickeln immer neue Methoden, um Systeme zu kompromittieren, sei es durch Malware, gezielte Phishing-Angriffe oder über Schwachstellen in der Infrastruktur. Als zentrale Komponente vieler moderner Sicherheitsarchitekturen gibt Ihnen Wazuh die Werkzeuge an die Hand, um in diesem Kampf nicht nur mitzuhalten, sondern einen Schritt voraus zu sein.

Wazuh kombiniert verschiedene Sicherheitsfunktionen wie Intrusion-Detection-Systeme (IDS), File Integrity Monitoring (FIM) und Vulnerability Management in einer einzigen Plattform. Diese Funktionen ermöglichen es, bösartige Aktivitäten frühzeitig zu erkennen, Systeme auf unautorisierte Änderungen zu überprüfen und potenzielle Schwachstellen zu identifizieren, bevor sie ausgenutzt werden können.

Wenn Sie jetzt denken: „Das klingt nach viel Technik – bin ich dem gewachsen? Dieses Buch führt Sie Schritt für Schritt. Es erklärt die Grundlagen, ohne zu tief in die technischen Details einzutauchen. Gleichzeitig bietet das Buch genug technische Tiefe, sodass auch erfahrene Administratoren und Sicherheitsexperten auf ihre Kosten kom-

men. Von der Installation der Wazuh-Umgebung über die Konfiguration bis hin zum Umgang mit realen Bedrohungen vermittelt Ihnen dieses Buch das nötige Wissen und Selbstvertrauen, um Wazuh erfolgreich in Ihrem Unternehmen einzusetzen oder für Ihre Weiterbildung zu nutzen.

Der Open-Source-Charakter von Wazuh bietet entscheidende Vorteile: Sie können die Plattform an Ihre speziellen Bedürfnisse anpassen, erhalten kontinuierliche Verbesserungen durch eine große Community und vermeiden hohe Lizenzkosten. Vor allem aber bietet es Ihnen die Flexibilität, Ihre Sicherheitsarchitektur ganz nach Ihren eigenen Anforderungen zu gestalten.

Mit Wazuh steht Ihnen eine Plattform zur Verfügung, die sowohl für große Unternehmen, kleinere IT-Abteilungen als auch für den privaten Gebrauch geeignet ist. Lassen Sie uns gemeinsam die vielfältigen Möglichkeiten von Wazuh entdecken – und wie es Ihnen helfen kann, Ihre IT-Sicherheit auf die nächste Stufe zu heben.

Lassen Sie sich trotz der Herausforderungen nicht entmutigen. Wazuh verfügt über eine ausgezeichnete Dokumentation, die Sie bei jedem Schritt unterstützt. Außerdem gibt es eine aktive und hilfsbereite Community, die Ihnen gerne weiterhilft, wenn Sie einmal nicht weiterkommen. Mit diesen Ressourcen sind Sie nie allein – auch wenn es manchmal schwierig erscheint, werden Sie schnell feststellen, dass sich die Mühe lohnt. Die Arbeit mit Wazuh wird Ihnen nicht nur technisches Wissen und wertvolle Erfahrungen vermitteln, sondern auch das Gefühl, Ihre IT-Sicherheit wirklich im Griff zu haben. Mit einer gesunden Portion Motivation und der richtigen Unterstützung werden Sie sehen, dass sich die Mühe lohnt.

Seien Sie mutig, seien Sie neugierig – und vor allem: Seien Sie bereit, Ihre IT-Sicherheit selbst in die Hand zu nehmen!

1.2 Ziel des Buches

In seinem Hauptwerk „Vom Kriege“ formulierte der preußische General Carl von Clausewitz die These, dass die Verteidigung die stärkere Form des Krieges ist.

„Achte in offenem Gelände wachsam auf deine Verteidigung, denn du musst mit einem Überraschungsangriff rechnen.“, äußerte der chinesische Philosoph und Stratege Sunzi in seinem Werk „Die Kunst des Krieges“.

Die strategischen Lehren von Clausewitz und Sunzi lassen sich in hervorragender Weise auf den Schutz von Unternehmensnetzwerken übertragen. Die Hervorhebung einer gründlichen Vorbereitung und Planung unterstreicht die Notwendigkeit einer umfassenden Sicherheitsstrategie, die regelmäßige Risikobewertungen, Schwachstellenanalysen und die Erstellung von Notfallplänen umfasst. In diesem Zusammenhang spielt die Schulung der Mitarbeiter eine zentrale Rolle, um die Cybersicherheit zu einer Priorität im gesamten Unternehmen zu machen.

Die Strategen weisen auch auf die Bedeutung von Wissen und Information hin, die sich direkt auf die IT-Sicherheit übertragen lassen. Eine genaue Kenntnis der eigenen Netzwerkinfrastruktur, kombiniert mit dem Einsatz von Threat Intelligence und Echtzeitanalysetools, ermöglicht es Unternehmen, Bedrohungen frühzeitig zu erkennen und darauf zu reagieren. Die kontinuierliche Weiterbildung des IT-Sicherheitsteams ist dabei unerlässlich, um mit der sich ständig verändernden Bedrohungslage Schritt zu halten. Nur wer seine Systeme aktiv überwacht und verteidigt, hat eine Chance, in der immer komplexer und dynamischer werdenden IT-Landschaft zu bestehen. Genau das ist der Ansatz dieses Buches: Ihnen zu zeigen, wie eine effektive Verteidigung in der IT aussehen kann – mit Wazuh als zentralem und kostenlosem Werkzeug.

Das Ziel dieses Buches ist es, Ihnen nicht nur die Grundlagen des Netzwerk-Monitorings und der Sicherheitsüberwachung zu vermitteln, sondern auch ein tieferes Verständnis für die Arbeit hinter der Technologie zu schaffen. Monitoring ist weit mehr als nur das bloße Sammeln von Daten; es geht darum, Risiken zu erkennen, potenzielle Bedrohungen zu analysieren und auf Basis fundierter Informationen zu handeln. Sie werden lernen, wie Sie Wazuh einsetzen, um diese Prozesse zu automatisieren und zu optimieren. Doch genauso wichtig ist es, ein Bewusstsein für die tägliche Arbeit und die Aufgaben, die mit der Implementierung eines solchen Systems verbunden sind, zu entwickeln.

Dabei ist Wazuh als Open-Source-Plattform Chance und Herausforderung zugleich. Die Vorteile liegen auf der Hand: Die Software ist flexibel, anpassbar und frei zugänglich. Sie profitieren von einer aktiven Community und der Möglichkeit, die Konfiguration selbst anzupassen. Doch genau diese Offenheit birgt auch einige Hürden. Sie erfordert ein hohes Maß an Eigeninitiative, technischer Kompetenz und kontinuierlichem Lernen. Die Konfiguration und Anpassung von Open-Source-Tools kann zeitaufwendig sein und der Weg ist nicht immer auf Anhieb klar. Doch gerade die Auseinandersetzung mit der Materie sorgt dafür, dass man nicht nur theoretisches Wissen anhäuft, sondern dieses auch direkt in der Praxis anwenden und damit festigen kann.

Ständige Weiterbildung ist in der Cybersicherheit unerlässlich. Die Bedrohungen entwickeln sich ständig weiter, und um auf dem neuesten Stand zu bleiben, müssen auch Sie sich ständig weiterbilden. Dies geschieht am besten durch praktische Übungen und die direkte Arbeit mit Systemen wie Wazuh. Theorie allein reicht nicht aus – das Verständnis für Cybersicherheit wächst, wenn man die Werkzeuge selbst in die Hand nimmt und lernt, sie zu beherrschen. Genau hier setzt dieses Buch an: Es begleitet Sie durch praktische Beispiele und reale Anwendungsszenarien, um Sie fit für die täglichen Herausforderungen des IT-Sicherheitsmonitorings zu machen.

Wazuh kann zu einem wichtigen Bestandteil Ihres Verständnisses von Cybersicherheit werden. Die Plattform bietet Ihnen nicht nur Werkzeuge zur Überwachung und Abwehr von Angriffen, sondern auch tiefe Einblicke in die Mechanismen, die hinter diesen Angriffen stecken.

Indem Sie die praktische Arbeit mit Wazuh und die ständige Auseinandersetzung mit aktuellen Entwicklungen in der Cybersicherheit verbinden, legen Sie den Grundstein für eine erfolgreiche Verteidigung Ihrer Systeme – und damit für den Gesamterfolg Ihrer IT-Sicherheit.

1.3 Wer soll das Buch lesen?

Dieses Buch richtet sich an eine breite Zielgruppe, die alle eines gemeinsam haben: das Interesse an IT-Sicherheit und den Wunsch, ihre Systeme besser zu schützen oder zu verstehen, wie Angriffe erkannt und verhindert werden können. Im Folgenden erfahren Sie, was die verschiedenen Lesergruppen aus diesem Buch lernen können:

IT-Fachleute: Für IT-Fachleute, die bereits über fundierte technische Kenntnisse verfügen, bietet dieses Buch die Möglichkeit, ihre Kenntnisse im Bereich der Netzwerküberwachung und Bedrohungserkennung zu vertiefen. Sie erfahren, wie sie Wazuh in bestehende IT-Infrastrukturen integrieren, die Konfiguration optimieren und spezifische Sicherheitsmodule anpassen können, um Bedrohungen in Echtzeit zu erkennen und zu neutralisieren.

Studierende der Cybersicherheit: Für Studierende bietet dieses Buch eine wertvolle praktische Ergänzung zur Theorie. Sie lernen nicht nur die Grundlagen der Überwachung und Sicherheitsanalyse, sondern auch, wie diese Konzepte in der realen Welt angewendet werden. Die praktischen Anleitungen und Fallstudien ermöglichen es ihnen, die in den Vorlesungen erlernten theoretischen Konzepte in die Praxis umzusetzen und ein tiefes Verständnis für moderne Sicherheitslösungen zu entwickeln.

Privatanwender, die sich für die Sicherheit ihrer Umgebung interessieren: Auch Privatanwender, die sich für die Sicherheit ihrer Systeme interessieren, können von diesem Buch profitieren. Wazuh kann nicht nur in Unternehmensumgebungen, sondern auch in privaten Netzwerken eingesetzt werden. Dieses Buch zeigt Ihnen, wie Sie Ihre persönlichen Geräte überwachen und absichern können, indem Sie potenzielle Bedrohungen frühzeitig erkennen und darauf reagieren – ohne teure kommerzielle Lösungen zu benötigen.

Penetrationstester: Für Penetrationstester, die ihre Fähigkeiten erweitern möchten, bietet dieses Buch wertvolle Einblicke in Abwehrstrategien. Es zeigt Ihnen, wie Sicherheitsteams Tools wie Wazuh einsetzen, um Angriffe zu erkennen. So können Sie Ihre eigenen Techniken verfeinern und besser verstehen, wie Sie Tests so gestalten können, dass sie realistischer und anspruchsvoller sind, und ob Ihre Angriffe möglicherweise in einem frühen Stadium abgefangen werden können.

Mitglieder von Red Teams: Für Mitglieder von Red Teams, die Angriffsszenarien entwickeln und dabei unerkannt bleiben wollen, ist dieses Buch ein Muss. Es hilft Ihnen zu verstehen, wie Sicherheitstools wie Wazuh funktionieren, welche Erken-

nungsmethoden eingesetzt werden und wie Sie Ihre Angriffstechniken weiterentwickeln können, um auch anspruchsvolle Sicherheitsmaßnahmen zu umgehen. Gleichzeitig bietet Ihnen das Buch wertvolle Einblicke, wie Sie bisher unentdeckte Schwachstellen finden können.

IT-Verantwortliche: Wenn Sie in Ihrem Unternehmen für die IT-Sicherheit verantwortlich sind, vermittelt Ihnen dieses Buch das nötige Wissen, um Ihre Netzwerke und Systeme effektiv zu überwachen und Schwachstellen zu identifizieren. Es zeigt Ihnen, wie Sie die Sicherheitsarchitektur Ihrer IT-Landschaft verbessern können, indem Sie Schwachstellen gezielt angehen, bevor sie ausgenutzt werden können. Wazuh hilft Ihnen dabei, potenzielle Gefahren zu erkennen, Bedrohungen zu priorisieren und geeignete Sicherheitsmaßnahmen zu ergreifen.

IT-Sicherheitsverantwortliche und interessierte Leser zur IT-Sicherheit und Datenschutz im Allgemeinen: Für IT-Sicherheitsverantwortliche, die über den Schutz einzelner Systeme hinausdenken und sich mit ganzheitlichen Sicherheits- und Datenschutzstrategien beschäftigen, ist dieses Buch eine wertvolle Ressource. Sie erfahren, wie Wazuh als zentrales Werkzeug in der Sicherheitsarchitektur eingesetzt werden kann, um eine umfassende Überwachung und Bedrohungserkennung zu gewährleisten. Wazuh unterstützt Sie nicht nur bei der Erkennung von Sicherheitsvorfällen, sondern auch bei der Überwachung der Einhaltung von Datenschutzanforderungen wie der DSGVO. Durch die Verknüpfung von Sicherheitsereignissen mit Compliance-Anforderungen können Sie sicherstellen, dass Ihr Unternehmen nicht nur vor Cyberangriffen geschützt ist, sondern auch gesetzliche Auflagen erfüllt. Datenschutz spielt in der modernen IT-Landschaft eine immer größere Rolle. Mit Wazuh können Sie sensible Daten überwachen und sicherstellen, dass alle Zugriffe transparent und nachvollziehbar sind. Dabei unterstützt das System die Integration mit anderen Datenschutz- und Compliance-Tools, sodass Sie einen ganzheitlichen Überblick über Ihre Sicherheits- und Datenschutzmaßnahmen behalten.

Risikomanagement: Für alle Leserinnen und Leser, die sich mit IT-Sicherheit und Datenschutz beschäftigen, ist auch das Thema Risikomanagement von zentraler Bedeutung. Dieses Buch zeigt Ihnen, wie Sie Risiken erkennen, bewerten und minimieren können. Sie lernen, Bedrohungen zu priorisieren und entsprechend zu handeln, bevor sie zu einem ernsthaften Problem werden. Wazuh hilft Ihnen, nicht nur reaktiv auf Sicherheitsvorfälle zu reagieren, sondern proaktiv potenzielle Gefahren zu erkennen und präventive Maßnahmen zu ergreifen.

Unabhängig davon, zu welcher dieser Gruppen Sie gehören, wird Ihnen dieses Buch wertvolle Einblicke in die moderne Cybersicherheit und den Einsatz von Wazuh zur Überwachung und Verteidigung Ihrer Systeme geben.

1.4 Was erwartet Sie in diesem Buch?

In diesem Buch erwartet Sie eine strukturierte Einführung und Vertiefung in die Welt des Netzwerk-Monitorings mit Wazuh. Jedes Kapitel ist darauf ausgelegt, Ihnen sowohl theoretische Grundlagen als auch praktische Anwendungen zu vermitteln. Hier eine Übersicht, was Sie in den einzelnen Kapiteln erwartet:

Kapitel 1: Orientierung und Motivation

In diesem Kapitel wird beschrieben, warum es wichtig ist, sich mit diesem Thema zu befassen und welchen Herausforderungen man sich stellen muss, wenn man sich intensiv mit Cybersicherheit beschäftigen will. Es wird geklärt, für welchen Personenkreis das Buch interessant ist und wie es aufgebaut ist.

Kapitel 2: Grundlagen der Netzwerküberwachung

In diesem Kapitel werden die wesentlichen Grundlagen der Netzwerküberwachung behandelt. Themen wie Threat Intelligence, MISP und das MITRE ATT&CK Framework werden grundlegend behandelt. Außerdem erfahren Sie, was SIEM (Security Information and Event Management) und SOAR (Security Orchestration Automation, and Response) sind und wie sie in die Sicherheitsinfrastruktur integriert werden.

Kapitel 3: Eine eigene Testumgebung aufbauen

Hier lernen Sie, wie Sie eine eigene Testumgebung einrichten können, um praktische Erfahrungen mit Wazuh zu sammeln. Sie erhalten Anleitungen zur Installation und Konfiguration von Proxmox oder XCP-ng für die Erstellung virtueller Maschinen. Zudem wird erläutert, wie Sie ein separates Testnetzwerk aufsetzen oder eine Cloud-Lösung für Ihre Tests nutzen können.

Kapitel 4: Netzwerkmonitoring mit Wazuh

Dieses Kapitel führt Sie tief in die Welt von Wazuh ein. Sie lernen die Bestandteile von Wazuh kennen und wie Sie die Plattform installieren. Anschließend erfahren Sie, wie Sie Agenten auf Windows-, Linux- und macOS-Systemen einrichten, Endpoint Security implementieren und Threat Intelligence sowie Security Operations in Ihre Umgebung monitoren. Themen wie Cloud-Sicherheit und aktive Reaktionen auf Cyberbedrohungen werden ebenfalls behandelt.

Kapitel 5: Anwendungsfälle

Hier wird es praktisch: Sie erstellen eigene Abfragen, richten Decoder und eigene Regeln ein. Außerdem lernen Sie, wie Sie mit weiteren Tools die Effektivität Ihrer Überwachung steigern können. Zahlreiche Use Cases veranschaulichen typische Bedrohungsszenarien, die Sie mit Wazuh erkennen und beheben können, etwa Brute-Force-Angriffe, SQL-Injection-Angriffe, Malware-Erkennung oder das Monitoring von Docker-Containern und Firewall-Systemen wie pfSense.

Kapitel 6: Zusammenarbeit mit anderen Cyber-Sicherheitswerkzeugen

Im letzten Kapitel wird erläutert, wie Wazuh mit anderen Cybersicherheits-Tools zusammenarbeitet. Sie lernen Tools wie The Hive, Shuffle und Cortex kennen, die zusammen mit Wazuh eine leistungsstarke Sicherheitslösung bilden. Diese Tools helfen, Arbeitsabläufe zu automatisieren und die Erkennung von Bedrohungen zu verbessern.

Mit dieser Struktur führt Sie das Buch von den Grundlagen zu fortgeschrittenen Themen und ermöglicht Ihnen, das Gelernte direkt in einer praktischen Umgebung anzuwenden. Am Ende werden Sie nicht nur die Funktionsweise von Wazuh beherrschen, sondern auch ein tiefes Verständnis für Netzwerküberwachung und Cybersicherheit entwickeln.

1.5 Wie ist das Buch aufgebaut

Nach einer Einführung in die grundlegenden Konzepte und Fachbegriffe werden Sie Schritt für Schritt durch den praktischen Einsatz von Wazuh und die Einrichtung einer Testumgebung geführt. Im Laufe des Buches wird ein kleines Netzwerk aus virtuellen Maschinen aufgebaut, das sowohl Wazuh als auch verschiedene Betriebssysteme wie Windows, Linux und macOS enthält. Diese Testumgebung ermöglicht es Ihnen, Wazuh in einer realistischen Umgebung zu konfigurieren und zu verwenden, um den vollen Funktionsumfang der Plattform kennenzulernen.

Das Buch enthält zahlreiche Listings, die längere Kommandozeilen und Konfigurationsdateien darstellen. Aus Gründen der Übersichtlichkeit sind diese Auflistungen mit vorangestellten Zeilennummern versehen. Dies erleichtert das Nachvollziehen und stellt sicher, dass Sie bei der Arbeit an Ihrer eigenen Umgebung gezielt auf bestimmte Zeilen verweisen können.

```
1   <decoder name="synology-connection">
2     <program_name>Connection</program_name>
3   </decoder>
4
5   <decoder name="synology-connection">
6     <prematch>DS716PlusII</prematch>
7   </decoder>
8
9   <decoder name="synology-connection">
10    <parent>synology-connection</parent>
11    <regex type="pcre2">User\s\[(\w+)\]\sfrom\s\[(\d+\.\d+\.\d+\.\d+)]\s(\w+\s\
w+\s\w+\s\w+\s\w+\s\[DSM])\svia\s\[(\w+)]\s(.*)</regex>
12    <order>srcuser, srcip, status, protocol, extra_data</order>
13  </decoder>
```

Über das Buch verteilt finden Sie verschiedene Kästen, die Ihnen zusätzliche Informationen bieten:

Hinweisboxen geben Ihnen nützliche Zusatzinformationen oder verweisen auf weiterführende Themen.

Praxistipps geben Ihnen praktische Hinweise, wie Sie typische Aufgaben schneller und effizienter erledigen können. Typische Fehler zeigen Ihnen häufige Stolpersteine auf und geben Hinweise, wie Sie diese vermeiden können.

Um sicherzustellen, dass Sie den behandelten Stoff auch wirklich verstanden haben, finden Sie am Ende jedes Abschnitts Kontrollfragen. Diese Fragen helfen Ihnen, das neu erworbene Wissen zu überprüfen und anzuwenden. Die Antworten auf diese Fragen finden Sie am Ende des Buches, wo sie mit kurzen Erläuterungen versehen sind, um Ihnen ein tieferes Verständnis des Inhalts zu ermöglichen.

Frage 3: Wer hat die Cyber Kill Chain entwickelt?

A) Lockheed Martin

B) MITRE Corporation

C) Symantec

D) Cisco Systems

Durch diesen Aufbau führt Sie das Buch sowohl theoretisch als auch praktisch in die Welt der Netzwerküberwachung mit Wazuh ein. Sie können das Gelernte direkt in Ihrer eigenen Testumgebung anwenden und erhalten durch die Listings und Boxen wertvolle Hilfestellungen, um erfolgreich mit Wazuh zu arbeiten.

1.6 Was Sie noch wissen sollten

Bevor Sie sich in dieses Buch vertiefen, sollten Sie wissen, dass Sie ein gewisses Maß an technischem Verständnis mitbringen müssen, um den vollen Nutzen aus dem Inhalt ziehen zu können. Dazu gehört ein solides Verständnis der drei wichtigsten Betriebssysteme: Windows, Linux und macOS. Dazu gehören grundlegende administrative Aufgaben, Dateimanagement und die Fähigkeit, einfache Fehler zu beheben. Ferner wird erwartet, dass die Leserinnen und Leser in der Lage sind, Schwachstellen in Systemen und Anwendungen zu erkennen und zu verstehen, um mögliche Angriffsflächen zu identifizieren.

Darüber hinaus sind grundlegende Programmierkenntnisse erforderlich, insbesondere in den Skriptsprachen Bash und PowerShell. Diese sind unerlässlich, um administrative Aufgaben zu automatisieren und Systeme effizient über die Kommandozeile zu administrieren. Auch der Umgang mit SSH und RDP wird vorausgesetzt, um einen sicheren Fernzugriff auf die eingesetzten Systeme zu erhalten. Docker wird verwendet, um Anwendungen in isolierten Containern zu paketieren, bereitzustellen und auszuführen.

Ein weiteres wichtiges Thema ist das Verständnis virtueller Umgebungen. Der Leser sollte wissen, was virtuelle Umgebungen sind, wie man sie einrichtet und welche Rolle sie bei der Isolierung und Verwaltung von Workloads oder Diensten in einem Netzwerk spielen. Schließlich wird betont, dass Geduld und Problemlösungsfähigkeiten unerlässlich sind. Da viele Aufgaben im Bereich der IT-Sicherheit komplex sind, sollten die Leserinnen und Leser darauf vorbereitet sein, bei der Fehlersuche und Fehlerbehebung Ausdauer an den Tag zu legen, da nicht immer alles beim ersten Mal funktioniert.

In diesem Buch habe ich künstliche Intelligenz (KI) eingesetzt, um den Schreibprozess effizienter zu gestalten. Die KI hat mir geholfen, Inhalte zu strukturieren, Texte zu überarbeiten und Recherchen zu beschleunigen. Sie lieferte mir Formulierungsvorschläge und half mir, Ideen weiterzuentwickeln.

Die Rolle der KI war jedoch rein unterstützend. Die eigentliche Konzeption des Buches, die Entwicklung der Argumente und die kreative Ausarbeitung der Themen basieren auf meinem eigenen Wissen und meiner Erfahrung als Cyberspezialist und Autor. Die KI konnte wertvolle Hilfestellungen geben, aber sie war nicht in der Lage, das Buch alleine zu schreiben. Der kreative Prozess, die Entscheidung über den Inhalt und die Feinabstimmung der Texte lagen letztlich in meiner Verantwortung.

In einigen Abschnitten des Buches werden Sie selbst den „schwarzen Hut“ aufsetzen und in die Rolle des Angreifers schlüpfen. Es ist jedoch wichtig zu betonen, dass Angriffe auf eigene Systeme, wie sie im Rahmen von Sicherheitstests durchgeführt werden, immer autorisiert sein müssen. Ohne ausdrückliche Erlaubnis und Zustimmung des Eigentümers sind solche Tests illegal und können schwerwiegende rechtliche Konsequenzen nach sich ziehen. Solche Tests sollten niemals in Produktionsumgebungen durchgeführt werden, da dies die Verfügbarkeit und Integrität kritischer Systeme gefährden kann. Stattdessen sollten sichere Testumgebungen verwendet werden, um das Risiko für den laufenden Betrieb zu minimieren.

1.7 Etwas zur verwendeten Sprache und Gendergerechtigkeit

Ich habe mich bemüht, die komplexen Inhalte rund um Wazuh in möglichst verständlichen und übersichtlichen Sätzen darzustellen. Mein besonderer Dank gilt dem Lektorat, das mich bei der Erstellung des Buches tatkräftig unterstützt hat.

Bitte haben Sie Verständnis dafür, dass das Buch viele englische Fachbegriffe enthält. Dies liegt daran, dass diese Begriffe in der IT-Sicherheit weit verbreitet sind und zum internationalen Fachvokabular gehören. Zwei Beispiele sollen dies verdeutlichen:

Der Begriff „Detection“ wird in Wazuh verwendet, um das Erkennen von sicherheitsrelevanten Ereignissen zu beschreiben. Eine deutsche Übersetzung wie „Erkennung“ wäre zwar möglich, aber der englische Begriff ist in der Praxis deutlich gebräuchlicher und wird international besser verstanden. Ein weiteres Beispiel ist der Begriff „Alert“, der im Kontext der Sicherheitsüberwachung verwendet wird, um auf bestimmte sicherheitsrelevante Ereignisse aufmerksam zu machen. Hier könnte man von einer „Warnung“ sprechen. Aber auch dieser englische Begriff ist in der Praxis gebräuchlich und wird in vielen Tools und Dokumentationen verwendet.

Ebenso wie bei der Wahl der Fachbegriffe auf Verständlichkeit und Praxisnähe geachtet wurde, war es mir wichtig, eine geschlechtergerechte Sprache zu verwenden. Die Verwendung einer geschlechtsspezifischen Formulierung wird von vielen Leserinnen und Lesern erwartet. In diesem Buch werden jedoch vorrangig geschlechtsneutrale Bezeichnungen verwendet. Soweit im Text geschlechtsspezifische Bezeichnungen verwendet werden, beziehen sich diese selbstverständlich auf alle Geschlechter gleichermaßen und dienen ausschließlich der besseren Lesbarkeit.

Abschließend sei darauf hingewiesen, dass ich bei der Verwendung von Farbbezeichnungen wie „Whitelist“ oder „Blacklist“ ausdrücklich betone, dass diese Begriffe keinerlei Bezug zu menschlicher Hautfarbe oder Diskriminierung haben. Solche Begriffe sind historisch gewachsen und dienen in der IT lediglich dazu, technische Konzepte einfach und verständlich darzustellen. Jegliche Form der Diskriminierung, sei es aufgrund der Hautfarbe, der Herkunft oder des Geschlechts, lehne ich entschieden ab. Ich bitte daher die Leserinnen und Leser, diese Fachbegriffe ausschließlich im technischen Kontext zu betrachten.

2
Grundlagen der Netzwerküberwachung

2.1 Herausforderungen und Trends

Um die Notwendigkeit von Tools wie Wazuh oder ähnlichen Lösungen zu verstehen, lohnt sich ein Blick in die Geschichte der IT-Sicherheit und Netzwerküberwachung. Die Entstehung solcher Systeme ist eng mit der zunehmenden Komplexität und Verbreitung von Computernetzwerken und der wachsenden Bedrohung durch Cyberangriffe verbunden.

In den Anfängen der IT, als die Netzwerke noch klein und überschaubar waren, reichten einfache Sicherheitsmaßnahmen wie Firewalls und Antivirenprogramme aus, um die Systeme zu schützen. Mit der rasanten Entwicklung des Internets und der zunehmenden Vernetzung von Unternehmen stieg jedoch auch die Gefahr, dass Angreifer Schwachstellen in Systemen ausnutzen. Hacker entwickelten immer raffiniertere Methoden, um in Netzwerke einzudringen, Daten zu stehlen oder Systeme lahmzulegen. In den 1990er-Jahren wurde deutlich, dass traditionelle Sicherheitswerkzeuge allein nicht ausreichten, um diese komplexen Bedrohungen zu erkennen und abzuwehren. Es entstand die Notwendigkeit, die Aktivitäten in Netzwerken genauer zu überwachen, um Anomalien und verdächtiges Verhalten frühzeitig zu erkennen. So wurden die ersten Intrusion-Detection-Systeme (IDS) entwickelt. Diese Werkzeuge überwachten den Netzwerkverkehr und suchten nach bekannten Angriffsmustern, um bei verdächtigen Aktivitäten Alarm zu schlagen.

Mit der Zeit entstand das Bedürfnis, nicht nur einzelne Vorfälle zu erkennen, sondern ein umfassendes Bild der gesamten Sicherheitslage eines Unternehmens zu erhalten. Hier kamen Systeme zur Security Information and Event Management (SIEM) ins Spiel. Diese Systeme wie Splunk, IBM QRadar oder ArcSight von OpenText sammelten und korrelierten Logdaten aus verschiedenen Quellen im Netzwerk wie Servern, Firewalls, Datenbanken und Anwendungen. Sie ermöglichten es Sicherheitsteams, in

Echtzeit auf Bedrohungen zu reagieren, indem sie verdächtige Aktivitäten im gesamten Netzwerk verfolgten und analysierten.

Wazuh [1] ist als Open-Source-SIEM-Tool ein relativ neuer Akteur in diesem Bereich, aber seine Wurzeln und die Motivation für seine Entwicklung lassen sich auf ähnliche Herausforderungen zurückführen, mit denen sich andere SIEM-Systeme konfrontiert sahen. Wazuh entstand aus dem Bedarf an einem flexiblen, leicht anpassbaren und erschwinglichen Tool, das Sicherheitsüberwachung auf Unternehmensebene bietet, ohne die Einschränkungen vieler kommerzieller Lösungen. Die Entwickler von Wazuh wollten eine Lösung schaffen, die es Unternehmen ermöglicht, Sicherheitsbedrohungen schnell zu erkennen, Compliance-Anforderungen zu erfüllen und ein transparentes, anpassbares Sicherheitssystem zu implementieren. Dabei sollte die Community eine zentrale Rolle spielen, indem sie kontinuierlich Feedback gibt und zur Weiterentwicklung des Tools beiträgt. Wazuh kombiniert moderne Ansätze wie Host-basierte Intrusion Detection, File Integrity Monitoring und Schwachstellenüberwachung in einem einzigen Framework.

Zusammenfassend lässt sich sagen, dass die Entwicklung von Netzwerküberwachungs- und SIEM-Tools wie Wazuh eng mit dem wachsenden Bedarf an umfassender Sicherheit und Bedrohungserkennung in komplexen, vernetzten IT-Umgebungen zusammenhängt. Angesichts immer raffinierterer Angriffstechniken und der wachsenden Bedeutung von IT-Sicherheit wird die Weiterentwicklung solcher Tools auch weiterhin eine zentrale Rolle spielen.

Bei der Weiterentwicklung von SIEM-Systemen lassen sich mehrere wichtige Richtungen erkennen. Ein zentraler Trend ist die zunehmende Integration von künstlicher Intelligenz und maschinellem Lernen. So wurde beispielsweise Falcon Next-Gen SIEM [2] von CrowdStrike von Grund auf für die Integration und Nutzung von KI entwickelt. Es ist darauf ausgelegt, KI-Modelle und -Algorithmen nahtlos in den gesamten Sicherheitsprozess einzubinden. Diese Technologien ermöglichen es SIEM-Systemen, komplexe Muster in Echtzeit zu erkennen und potenzielle Bedrohungen mit höherer Genauigkeit zu identifizieren. Dadurch wird die Zahl der Fehlalarme reduziert und die Effizienz der Sicherheitsanalysten erhöht.

Ein weiterer wichtiger Trend ist die Verlagerung von SIEM-Lösungen in die Cloud [3]. Cloud-basierte SIEM-Systeme bieten eine höhere Skalierbarkeit und Flexibilität, was insbesondere für Unternehmen mit wachsenden oder schwankenden Datenmengen von Vorteil ist. Zudem ermöglichen sie eine einfachere Integration mit anderen Cloud-Diensten und -Anwendungen.

Auch die Automatisierung von Sicherheitsprozessen gewinnt zunehmend an Bedeutung. Moderne SIEM-Systeme integrieren zunehmend Security Orchestration, Automation and Response (SOAR) Funktionalitäten, um Routineaufgaben zu automatisieren und die Reaktionszeit auf Sicherheitsvorfälle zu verkürzen. Dabei sind die Entwickler bestrebt, die Benutzerfreundlichkeit und die Visualisierung der Ergebnisse kontinuierlich zu verbessern. SIEM-Anbieter arbeiten daran, ihre Lösungen intuitiver

zu gestalten und komplexe Sicherheitsdaten in leicht verständlichen Dashboards und Berichten darzustellen. Dies erleichtert es auch technisch weniger versierten Mitarbeitern, Sicherheitsanalysen durchzuführen und fundierte Entscheidungen zu treffen.

Nicht zuletzt gewinnt die Integration von Threat Intelligence an Bedeutung. SIEM-Systeme nutzen zunehmend externe Bedrohungsdaten, um proaktiv auf neue und aufkommende Bedrohungen reagieren zu können. Diese Integration ermöglicht es Unternehmen, ihre Abwehrmaßnahmen kontinuierlich an die sich ständig verändernde Bedrohungslandschaft anzupassen.

Die Entwicklung von SIEM-Systemen spiegelt somit die zunehmende Komplexität der Cyber-Sicherheitslandschaft wider. Anbieter und Unternehmen müssen agil und innovativ bleiben, um mit den sich ständig verändernden Bedrohungen Schritt zu halten und eine robuste Verteidigung gegen Cyberangriffe zu gewährleisten.

Links zu Hintergrundinformationen und Downloads:

[1] Wazuh – The Open Source Security Platform Blog – *https://wazuh.com/blog*

[2] CrowdStrike Falcon SIEM – *https://www.crowdstrike.de/platform/next-gen-siem*

[3] Wazuh – Cloud protection – *https://wazuh.com/cloud*

2.2 Was ist ein SIEM?

Ein SIEM (Security Information and Event Management) [1] ist ein System, das Unternehmen dabei hilft, ihre IT-Sicherheit zu überwachen, Bedrohungen zu erkennen und auf Sicherheitsvorfälle zu reagieren. Es sammelt und analysiert Daten aus verschiedenen Teilen eines Netzwerks, um potenziell verdächtige Aktivitäten oder Angriffe zu identifizieren. SIEMs sind besonders hilfreich, weil sie viele Informationen an einem zentralen Ort zusammenführen und Sicherheitsteams dabei unterstützen, Probleme schnell zu erkennen und darauf zu reagieren.

Ein SIEM besteht im Allgemeinen aus mehreren Hauptkomponenten:

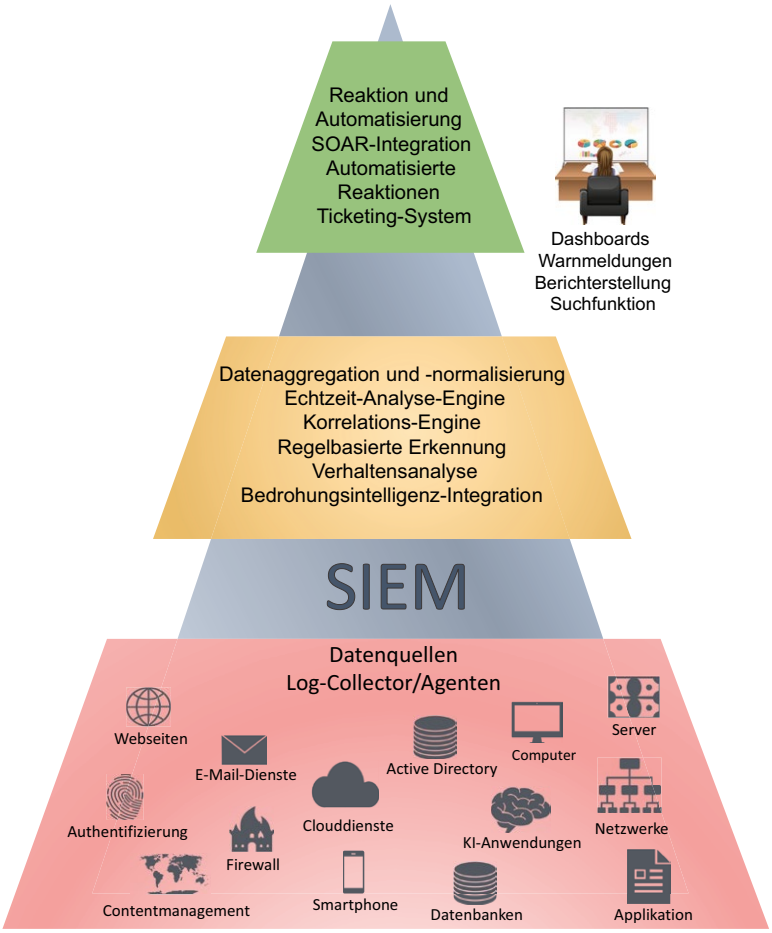

Bild 2.1 Hauptkomponenten eines SIEM

Datenquelle:

Datenquellen sind der Ausgangspunkt für jedes SIEM-System. Sie umfassen eine Vielzahl von Geräten und Systemen innerhalb eines Unternehmens, die sicherheitsrelevante Informationen in Form von Logdaten liefern. Typische Datenquellen sind Firewalls, Server, Anwendungen, Netzwerkgeräte und Endpunkte wie PCs, Laptops oder mobile Geräte. Firewalls liefern beispielsweise wichtige Informationen über den Netzwerkverkehr und blockierte Verbindungen, während Server Logs über Anmeldeversuche, Systemfehler oder Sicherheitsvorfälle bereitstellen. Anwendungen erzeugen Protokolle, die zeigen, welche Funktionen von welchen Benutzern verwendet wurden, und Netzwerkgeräte wie Router oder Switches dokumentieren den Daten-