2025

Lagebericht Observability

Der Aufstieg eines neuen Wachstumstreibers

splunk>
a CISCO company

Inhaltsverzeichnis

Vorwort der Geschäftsführung

Als ich vor über zehn Jahren mit Observability anfing, war unsere Aufgabe einfach: Services und Systeme am Laufen halten. Überschauen, was vor sich geht und wer betroffen ist, das Problem eingrenzen und beheben. Heute ist es so, dass Software das Geschäft nicht nur unterstützt – sie *ist* das Geschäft.

Seit digitale Experience die primäre Kundeninteraktion ist, hat Observability an Reichweite gewonnen. Korrelierte Telemetriedaten und Geschäftsergebnisse sind eine wichtige Entscheidungsgrundlage, z. B. für Kundenbindung oder Produktentwicklung. Und während KI bereits die tektonischen Platten der IT-Welt verschiebt, fällt Observability Verantwortung auf einer neuen Ebene zu: das Monitoring komplexer, dynamischer KI-Workloads. Diese Evolution positioniert Observability nicht allein als Basis der Customer Experience, sondern als Enabler von KI-gestützter Innovation und geschäftlichem Wachstum.

Weil wir diesen Wandel besser verstehen und wissen wollten, was die stärksten Teams besonders auszeichnet, haben wir für den Lagebericht Observability 2025 insgesamt 1855 Fachleute aus ITOps und Engineering befragt. Eine Gruppe sticht besonders heraus, die mehr zum Geschäftsergebnis beiträgt als die übrigen. Diese Befragten arbeiten enger mit den Security-Teams zusammen, gehen Incidents strategischer an und investieren in zukunftsweisende Technologien und neuere Verfahren.

Observability-Verantwortliche sind heute in Planung und Entscheidungsfindung auf höchster Ebene eingebunden, sie bringen ihr Fachwissen (und ihre Daten) in die Strategien der Kundenbindung, bei Produkt-Roadmaps und in der Vorstandsetage ein. Sie tragen ihren Teil der Verantwortung – jetzt ist es Zeit, davon zu profitieren.

PCL

Patrick Lin
SVP und GM, Observability, Splunk

Kapitel 1

Observability wird Wachstumstreiber

Jedes kühne unternehmerische Unterfangen, jede Innovation beginnt mit einem zündenden Funken. Und es braucht einen Katalysator, der die Entwicklung anstößt und zielgerichtet am Laufen hält. Das kann die Marktforschung sein, die eine überraschende Erkenntnis vorlegt, z. B. dass eine bestimmte demografische Gruppe Ihr Produkt auf eine ganz unerwartete Art nutzt, was die Tore zu neuen Märkten öffnet. Oder es ist eine wenig beachtete Zusatzfunktion, die sich als Schlüssel zur Kundenbindung entpuppt – und plötzlich bekommt die Roadmap eine ganz neue Richtung.

Diese Sternstunden der Erkenntnis kommen nicht von ungefähr. Sie entstehen durch Kräfte, die zwar manchmal leise sind, doch letztlich entscheidend. Observability entwickelt sich gerade neu zu einer solchen Kraft. Und auch wenn Observability und die Erkenntnisse, die damit gewonnen werden, am Ende vielleicht nicht die Entscheidung treffen, so gilt doch: Was schnell und wichtig ist, wird erst durch Observability sichtbar.

Daten bringen Observability und Business zusammen

Unternehmen ist heute mehr denn je bewusst, dass Software-Entscheidungen weitreichende Konsequenzen haben, in Bezug auf die Customer Experience, die Markenwahrnehmung etc. Unternehmen nutzen Observability-Daten und beantworten damit die Frage „Wie können wir die Daten aus unseren Anwendungen für betriebswirtschaftliche Entscheidungen nutzen?“ Die alte Frage „Was ist kaputt?“ spielt eine eher untergeordnete Rolle.

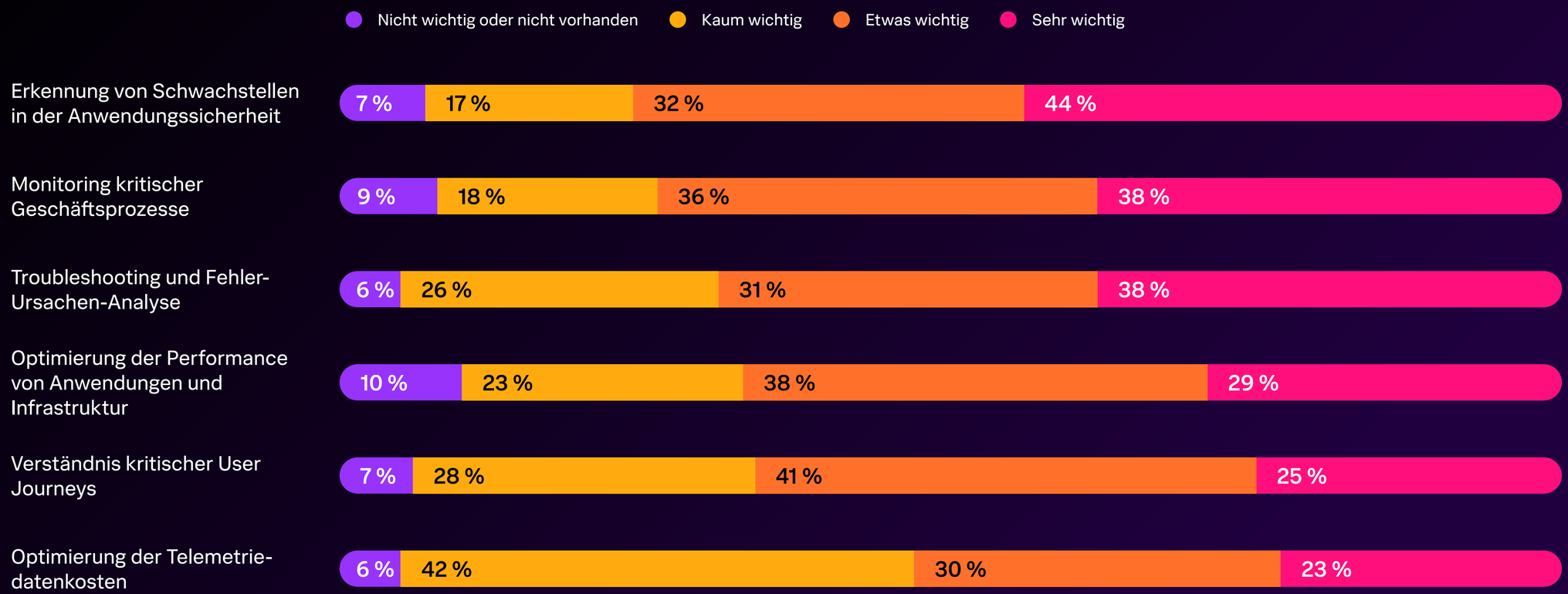
Weil diese Entscheidungen auf sicheren Beinen stehen sollen, ist die Erfassung von Geschäftsmetriken in der praktischen Observability mittlerweile eine der wichtigsten Prioritäten. Fast drei Viertel der Befragten (74 %) sagen, dass das Monitoring kritischer Geschäftsprozesse *einigermaßen wichtig* bis *sehr wichtig* ist. Diejenigen, die einen hohen ROI aus ihren Observability-Lösungen ziehen, legen sich bei diesem Punkt mit besonderem Nachdruck fest und wählen kritische Geschäftsprozesse häufiger als alle anderen Optionen – was bedeuten dürfte, dass dies bei ihnen die wichtigste Observability-Funktion ist.

Hat das Unternehmen ein sprunghaftes Umsatzplus zu verzeichnen, weil es eine neue Funktion herausgebracht hat oder weil das Marketing-Team eine geniale Kampagne gefahren hat? Früher war die Antwort nur mit viel Zeitaufwand, einem scharfen analytischen Auge und engelsgleicher Geduld herauszufinden. Heute ist Observability der Katalysator, der Anwendungstelemetrie in Business-Aktion umwandelt. Die Leute im Einsatz können anhand von Observability-Daten herausfinden, warum der Umsatz einbricht, wo es Reibungsverluste bei der Kundschaft gibt und wie die Produkt-Performance auf das Wachstum des Geschäfts wirkt.

Die Produktteams sollten eng mit dem Engineering zusammenarbeiten, sodass sie informierte Roadmap-Entscheidungen treffen und auf der Basis von Telemetrie-Erkenntnissen bestimmen können, welche Funktionen sie vorrangig behandeln sollten. Die Demokratisierung der Business-Daten ist der beste Weg, diesen Zauber Wirklichkeit werden zu lassen. Wenn die Teams darauf warten, dass ein Business-Analyst Daten von drei verschiedenen Dashboards abruft, haben sie den Zeitpunkt bereits verpasst.

— Greg Leffler, Director of Developer Evangelism, Splunk

Die betriebswirtschaftliche Bedeutung von Observability-Funktionen

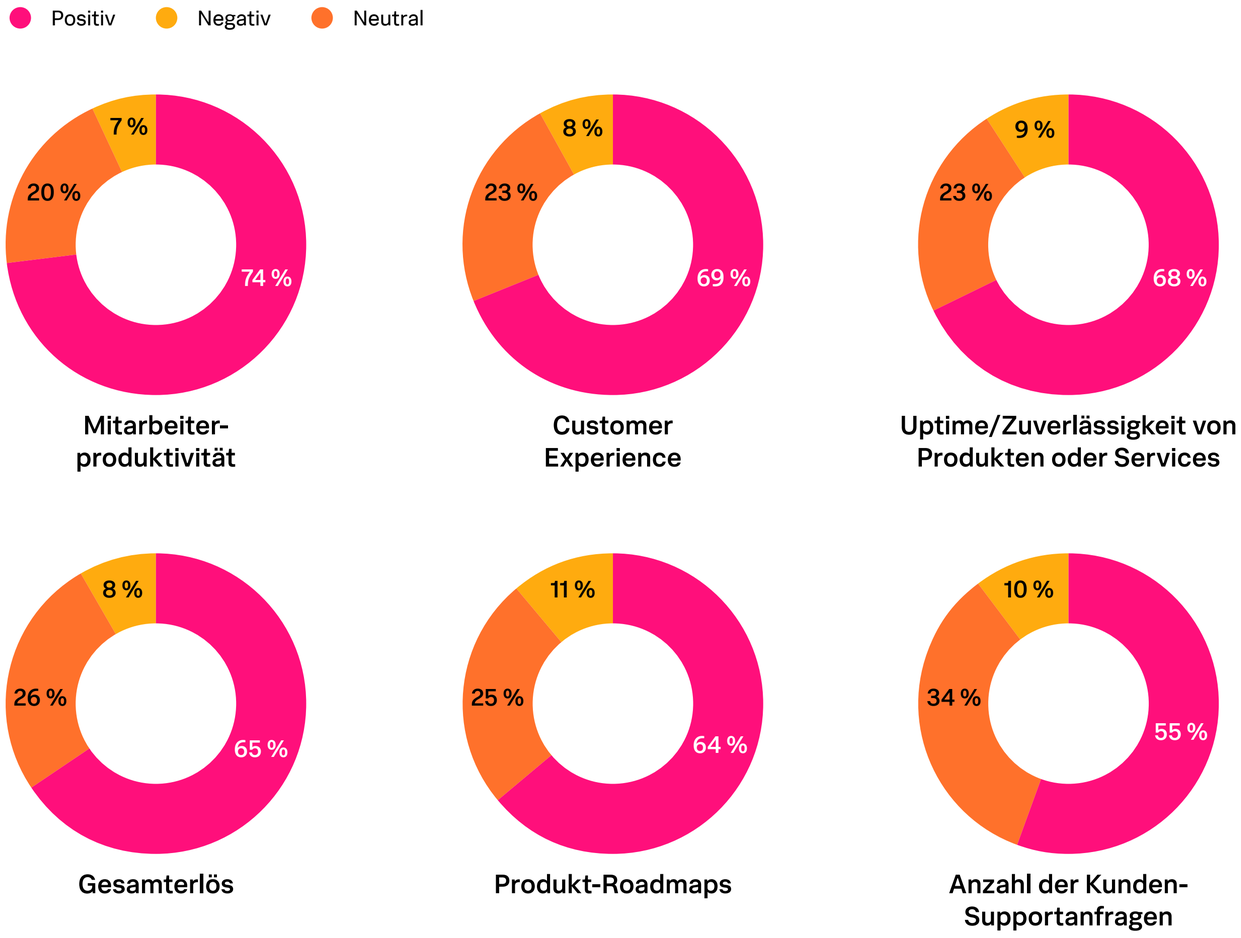


Rundungsbedingt ergeben die Anteile zusammen unter Umständen nicht genau 100 %.

Observability sollte nicht nur gründlichen Einblick in die Business-Metriken geben, sondern unmittelbar zu relevanten Ergebnissen wie schnellerer Leistung, besserer User Experience und höheren Erlösen beitragen. Wenn die Engineering- und ITOps-Teams mit belastbaren Metriken arbeiten, können sie sich auf Aufgaben konzentrieren, die direkt mit dem Geschäft zu tun haben: die entscheidenden User-Flows nachvollziehen, Echtzeit-Dashboards für Führungskräfte einrichten und dadurch die Technologie- und die Business-Strategie gleichermaßen prägen, Performance-Probleme bzw. Chancen der Anwendungen mit dem Umsatz korrelieren etc. Ein E-Commerce-Unternehmen kann z. B. dank Observability den gesamten Weg vom Besuch der Website bis zur Auftragsabwicklung visualisieren und Umsatzeinbußen verhindern, indem es sicherstellt, dass die betreffenden Business-Systeme verlässlich online bleiben. Es ist daher plausibel, dass 65 % der Befragten die Fähigkeit ihrer Observability-Lösung, kritische User-Journeys zu überschauen, *einigermaßen wichtig* bis *sehr wichtig* für das Gesamtgeschäft finden.

Diesen Anforderungen werden die Unternehmen auch gerecht: 65 % der Befragten geben an, dass sich ihre Observability-Praxis positiv auf den Umsatz auswirkt. Und 64 % sagen, dass sich ihre Observability-Praxis positiv auf die Produkt-Roadmaps auswirkt. Die Produktteams können anhand der Daten aus dem Real User Monitoring (RUM) nachvollziehen, wie lange es dauert, bis eine Seite vollständig gerendert ist, und wie schnell User mit der Seite interagieren, können diese Daten dann mit App-Performance-Metriken korrelieren und daraus ihre Schlussfolgerungen ziehen – z. B. kann es sein, dass die Performance ausgebremst wird und die Abbruchrate steigt, wenn die Website um neue Funktionen erweitert wird. Oder dass eine Softwareversion mit strengeren Schutzvorkehrungen gegen Betrug letztlich zu Umsatzeinbußen führt.

Wie sich Observability auf das Geschäft auswirkt



Rundungsbedingt ergeben die Anteile zusammen unter Umständen nicht genau 100 %.

Stressfrei durch den Observability-Alltag

Wenn Sie im Bereich ITOps oder Engineering arbeiten, kennen Sie diese Art von Tag: Er beginnt mit der schlimmsten Warnbenachrichtigung, die Sie sich denken können, eskaliert dann in einer Flut weiterer Meldungen und wird nur noch schlimmer, wenn Sie Ihre Vorgesetzten mit schlechten Nachrichten wecken müssen. Die ganze Zeit flüstert Ihnen ein leises Stimmchen zu: „Du bist erledigt." Und wenn Sie Glück haben, dann haben Sie am Ende des Tages die Flut aufgehalten – provisorisch, mit Ach und Krach, aber immer noch mit hohem Adrenalinspiegel.

Der Stress in solchen Situationen ist verständlich. Sie sind auch nur ein Mensch. Aber solche Panikmomente sollten bei der Incident Response nur selten auftreten. 21 % der Befragten geben an, dass sie *manchmal, oft* oder *immer* in Panik geraten, wenn ein Incident auftritt, der Folgen für die Kundschaft hat. Dabei ist selbst „manchmal" noch zu oft. Die Löscheinsätze im Notfall führen zu Burn-out und sind ein Zeichen dafür, dass die Teams sich abmühen, ohne den gesamten Kontext des Incidents zu kennen.

Solide Pläne statt geschäftiger Panik

Arbeit unter Druck gehört bei ITOps und Engineering dazu. Praktische Observability wird daran gemessen, welche Art von Incident-Reaktion damit möglich wird – und ob sich künftige Incidents verhindern lassen. Wenn die Alarmglocken schrillen und Katastrophenstimmung herrscht, ist es wichtig, dass die Teams ruhig und handlungssicher bleiben.

Runbooks, Reaktionspläne und Post-mortem-Analysen sind allesamt methodische, strategische Ansätze zur Panikvermeidung. Bei mehr als der Hälfte der Befragten (54 %) wird *oft* oder *immer* ein detaillierter Reaktionsplan entwickelt, und 71 % sagen, dass sie *oft* oder *immer* nach einem Incident eine detaillierte Überprüfung durchführen.

Außerdem gilt: Gemeinsam sind wir stark. Es ist beruhigend, wenn Sie wissen, dass Sie an vorderster Front nicht ganz allein stehen, sondern Kollegen zur Seite haben. Allerdings: Es gibt einen großen Unterschied zwischen strategischer Zusammenarbeit und diesem Alle-Mann-an-Deck-Aktionismus.

Krisenstäbe geraten leicht zu einer Panikküche, in der viele Köche den Brei verderben. Dann werden wertvolle Unternehmensressourcen verbrannt und wertvolle Team-Mitglieder verschwinden mit Untersuchungsaufträgen in Schwarzen Löchern.

„Wenn die Tools des Unternehmens nicht effektiv genug sind, um den Teams bei der Isolierung des Problembereichs zu helfen, dann werden Krisenstäbe zur Regel“, sagt Patrick Lin, SVP und GM Observability bei Splunk. „Die Observability-Software hat sich so weit entwickelt, dass die Teams in der Lage sein sollten, Services wiederherzustellen, ohne dass sie dazu 50 Leute holen müssen.“

Der klügere Ansatz besteht darin, den Incident einem bestimmten Team zuzuordnen und darauf zu vertrauen, dass das Team ihn löst – dies ist aber nur bei 22 % der Befragten *oft* oder *immer* der Fall. Ein solches Vorgehen ist ein Zeichen einer Observability-Praxis mit hohem Reifegrad und fortgeschrittenen Prozessen der Zusammenarbeit (darauf kommen wir weiter unten noch zu sprechen).

73%

haben bereits Ausfälle aufgrund von ignorierten oder unterdrückten Warnmeldungen erlebt

Post-mortem-Analysen ermöglichen einen förmlichen Abschluss, und das kann unglaublich kathartisch wirken. Die Gewissheit, dass sich ein Incident – egal wie angstauslösend er anfangs war – nicht wiederholen wird, wirkt Wunder für die psychische Gesundheit aller Beteiligten.

— Caitlin Halla, Developer Evangelist, Splunk

Fehlalarme und verzettelte Tools schaden der Moral und dem ROI

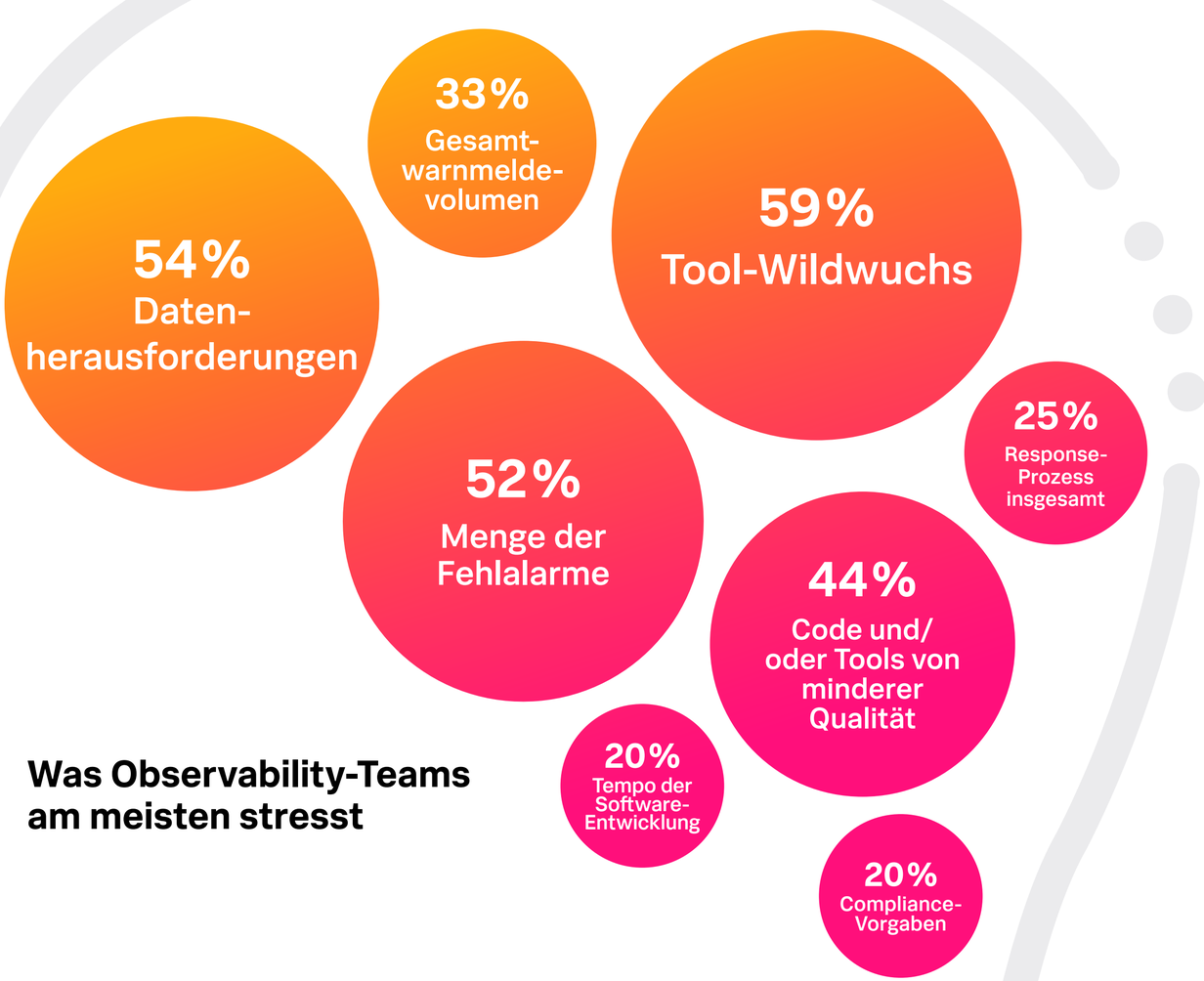
Incidents sind unbestritten stressig. Aber sie sind keineswegs der Faktor, der am heftigsten auf die psychische Gesundheit der Teams schlägt. Nur 25 % der Befragten sagen, dass sich die Incident-Reaktion negativ auf die Arbeitsmoral auswirkt. Dagegen ist bei 59 % die ausufernde Menge der Tools ein Grund zur Beunruhigung.

Dicht darauf folgt ein Problem, das ITOps- und Engineering-Teams seit Jahren plagt: die Menge der Fehlalarme. Beide Probleme hängen eng zusammen. Je mehr Tools ein Unternehmen im Einsatz hat, desto höher ist die Wahrscheinlichkeit, dass diese Tools Fehlalarme produzieren – vor allem dann, wenn die Teams so ausgelastet sind, dass sie keine Zeit haben, ihre Warnmelderegeln feinzustimmen, Signale systemübergreifend zu korrelieren und sich zu vergewissern, was wirklich wichtig ist.

Tool-Wildwuchs ist eine echte Herausforderung. Aber was den ROI wirklich nach unten zieht, ist die insgesamt schlechte Qualität der Erkennungen. Sind Warnmeldungen verrauscht, redundant oder ohne Kontext, können selbst die fortschrittlichsten Toolsets keinen sinnvollen Nutzen bringen.

— Stephanie Elsesser, Director of Observability Strategists, Splunk

Was Observability-Teams am meisten stresst



Die Befragten konnten eine Mehrfachauswahl treffen.

Fehlalarme bedeuten nicht nur Stress, sondern haben weitreichende Folgen und schlagen bis auf das Geschäftsergebnis durch. Mehr als die Hälfte der Befragten (54 %) gibt an, dass die Qualität ihrer Warnmelde-erkennungen einer der wichtigsten Faktoren für ihren Observability-ROI ist. Und 47 % sagen, dass Warnmeldungen einen *deutlichen* Einfluss auf die Sicherheitsentscheidungen in ihrem Unternehmen haben.

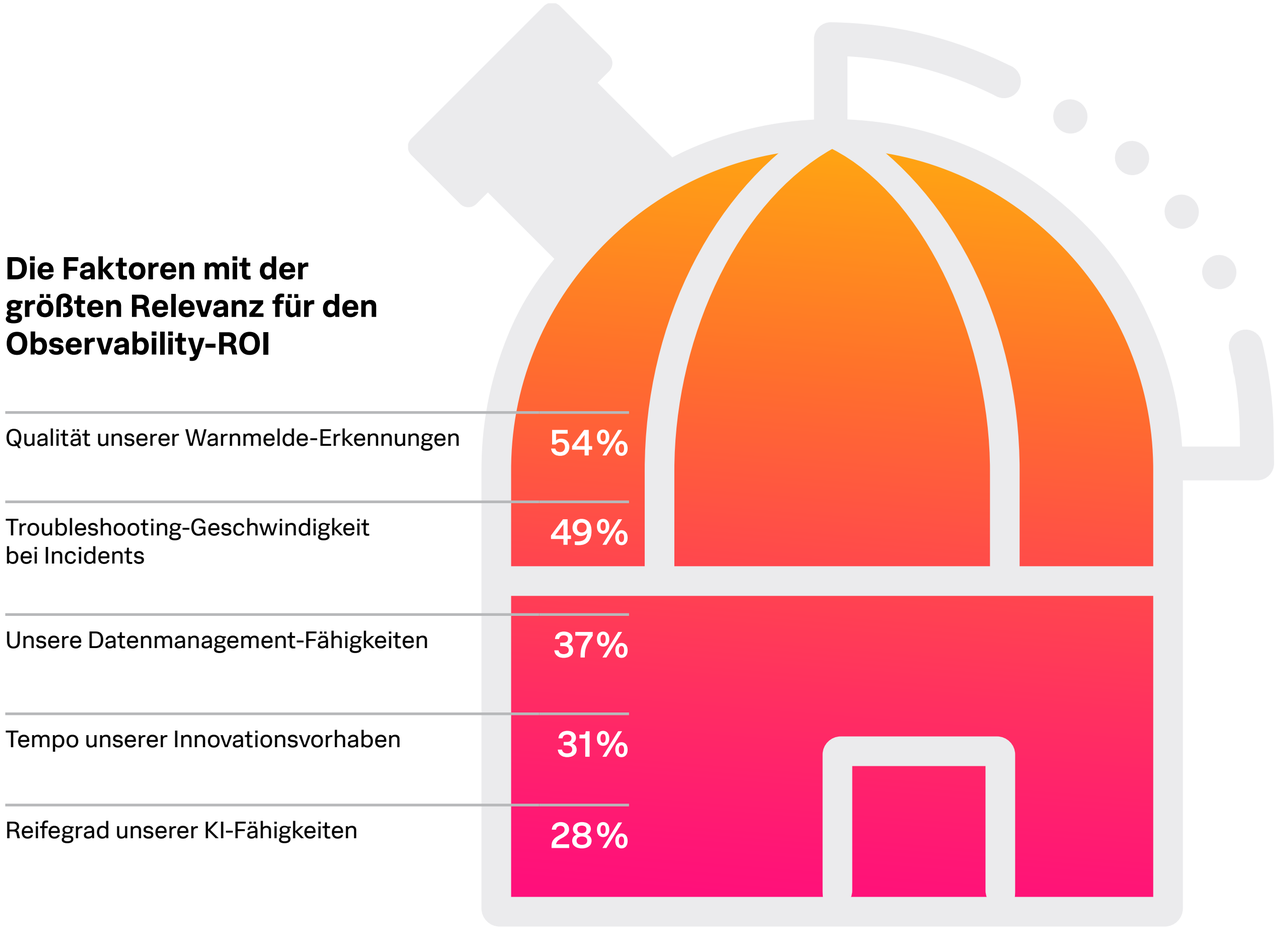
Im Bestreben, dem Rauschen der Fehlalarme zu entgehen, greifen einige Teams zu riskanten Methoden. 13 % gestehen ein, dass sie Warnmeldungen *oft* oder *immer* ignorieren bzw. ausblenden. Noch alarmierender ist die Tatsache, dass 73 % der Teams bereits Ausfälle aufgrund von ignorierten oder unterdrückten Warnmeldungen erlebt haben.

„Eine effektiv funktionierende Observability-Praxis sollte keine Warnmeldungen unterdrücken, Punkt“, sagt Greg Leffler. „Im Idealfall sollten Warnmeldungen nur bei unmittelbaren Problemen ergehen, die sich auf den Geschäftsgang auswirken.“

Klar ist, dass Warnmeldungen auf die Produktivität schlagen und für viele Fehlzeiten wegen mentaler Erschöpfung verantwortlich sind. 43 % der Befragten geben zu, dass sie „mehr Zeit als nötig“ mit der Bearbeitung von Warnmeldungen verbringen. Bei jeder Alert-Anzeige, egal wo, sehen Sie unten vermutlich einen ganzen Haufen ungelesener und unbearbeiteter Warnmeldungen. Das sollte zwar nicht sein, ist aber so. Eine Warnmeldung sollte eigentlich sofort Aufmerksamkeit erregen und genug Kontext mitbringen, dass die Teams rasch handeln können.

„Warnmeldungen werden immer eine zentrale Observability-Komponente sein“, sagt Mike Simon, Staff Developer Evangelist bei Splunk. „Wenn sie aber in größerem Umfang Handlungsgrundlage sein sollen, dann müssen Sie zusehen, dass Sie die Signalqualität verbessern und nicht nur das Rauschen reduzieren. Korrelieren Sie das, was relevant ist, überschauen Sie die Folgen für das Geschäft und heben Sie hervor, was wirklich Beachtung verdient, sodass die Teams im Ernstfall nachforschen können. So können Sie die vergeudete Zeit zurückgewinnen, und die Engineering-Teams können sich darauf konzentrieren, bessere Software zu entwickeln. Denn darauf kommt es am Ende an.“

Die Faktoren mit der größten Relevanz für den Observability-ROI



Die Befragten konnten eine Mehrfachauswahl treffen.

Kapitel 3

Zusammenarbeit mit Security erweitert den Observability-Wirkradius

Nehmen wir folgendes Szenario: Sie stellen fest, dass die Login-Latenzen in die Höhe schießen und dass die Last auf den Backend-Services der E-Commerce-Plattform Ihres Unternehmens stark zunimmt. Kunden lassen ihre Warenkörbe im Stich, überall ploppen Warnmeldungen auf und was am schlimmsten ist: Der Umsatz geht zurück. ITOps eskaliert das Problem ans Engineering, das auf die letzte Code-Version zurücksetzt – aber das Problem bleibt bestehen. Parallel dazu beginnt das Security-Team Untersuchungen auf potenziellen Bot-Traffic, hat das aber noch nicht als dringend eingestuft.

Jedes Team könnte auf eigene Faust vorgehen und dabei Zeit und Mühe verschwenden. Oder die Teams könnten alle gemeinsam Daten, Dashboards, Navigatoren und Kontext der Observability-Plattform nutzen und das Troubleshooting parallel vorantreiben. Zusammen könnten sie die Fehler-Ursachen schnell aufdecken – einen Credential-Stuffing-Angriff, der die Backend-Ressourcen ans Limit treibt – und das Problem schnell lösen, sodass die Kunden im besten Fall davon gar nichts mitbekommen.

Es zahlt sich aus, wenn Observability- und Security-Teams zusammenarbeiten. Fast zwei Drittel der Befragten (64 %) haben dann weniger Probleme mit der Performance von Anwendungen und Infrastruktur, 54 % verbessern ihre Datenqualität, und 54 % vertun weniger Zeit mit der Untersuchung von Problemen, was sich letztlich in besseren MTTD- und MTTR-Werten niederschlägt.

Von den Vorteilen der Zusammenarbeit profitiert das Geschäft insgesamt. 64 % sagen, dass es durch die Zusammenarbeit mit den Sicherheitsteams weniger Incidents gibt, von denen die Kundschaft etwas mitbekommt. Viele Unternehmen haben erkannt, dass der Wert von Observability-Daten nicht auf ITOps und Engineering beschränkt ist. Mehr als drei Viertel (76 %) geben an, dass die Fähigkeit ihrer Observability-Lösung, Schwachstellen und Bedrohungen der Anwendungssicherheit zu erkennen, für das Gesamtgeschäft ihres Unternehmens *einigermaßen wichtig* bis *sehr wichtig* ist.

Zusammenarbeit mit den Sicherheitsteams lohnt sich

In welchen Bereichen sich Vorteile aus der Zusammenarbeit ergeben

64 %
Weniger Incidents, von denen Kunden betroffen sind

64 %
Weniger Probleme mit der Performance von Anwendungen und Infrastruktur

54 %
Verbesserte Datenqualität

54 %
Weniger Zeit mit der Fehlersuche vergeudet

Die Befragten konnten eine Mehrfachauswahl treffen.

Weniger fortgeschrittene Sicherheits- und Observability-Teams haben ihre jeweils eigenen Tools und eigene Prioritäten und sie kommunizieren oft nur, wenn es absolut notwendig ist, in der Regel im Fall eines Incidents. Doch diese Grenzen von Daten, Tools und Kommunikation werden durchlässig. Eine Observability-Praxis, die nicht bereits Schritte unternommen hat, um diese Zusammenarbeit zu ermöglichen, wird abgehängt werden, insbesondere mit dem zunehmenden Einsatz von KI.

— Patrick Lin, SVP und GM Observability, Splunk

Partnerschaft ermöglicht schnellere Problemlösung

Kollaboration, Synergie, paralleles Arbeiten, klassische Teamarbeit – wie auch immer Sie es nennen: Die Zusammenarbeit mit den Sicherheitsteams ist ein bewusster, strukturierter Prozess, der etwas mehr verlangt als Observability-Daten einfach über den Zaun zu werfen und zu hoffen, dass sie auf fruchtbaren Boden fallen.

74 % der Befragten sagen, dass ihre Observability- und Sicherheitsteams Daten teilen und untereinander weiternutzen – ein grundlegender erster Schritt zur Zusammenarbeit. Zugleich geben 68 % an, dass beide Teams die gleichen Tools einsetzen.

Dies sollte heutzutage das Mindeste sein. Die Zusammenarbeit in Echtzeit fördert Kontext zutage, der mit Dashboards allein nicht zu bekommen ist. Nehmen wir an, dass das Engineering den API-Schlüssel eines Backend-Services ausgetauscht, aber einen vorgelagerten Service nicht auf die Verwendung des neuen Schlüssels aktualisiert hat. Nun schlagen beim Roll-out der neuen Version User-Anfragen fehl, was zu erneuten Versuchen und letztlich zu höheren Latenzen führt. Damit solche Zusammenhänge sichtbar werden, müssen die Daten der Latenzspitzen mit den Security-Logs nachbelichtet werden – und das ist eine Korrelationsebene, die in den meisten Observability-Dashboards gar nicht vorgesehen ist.

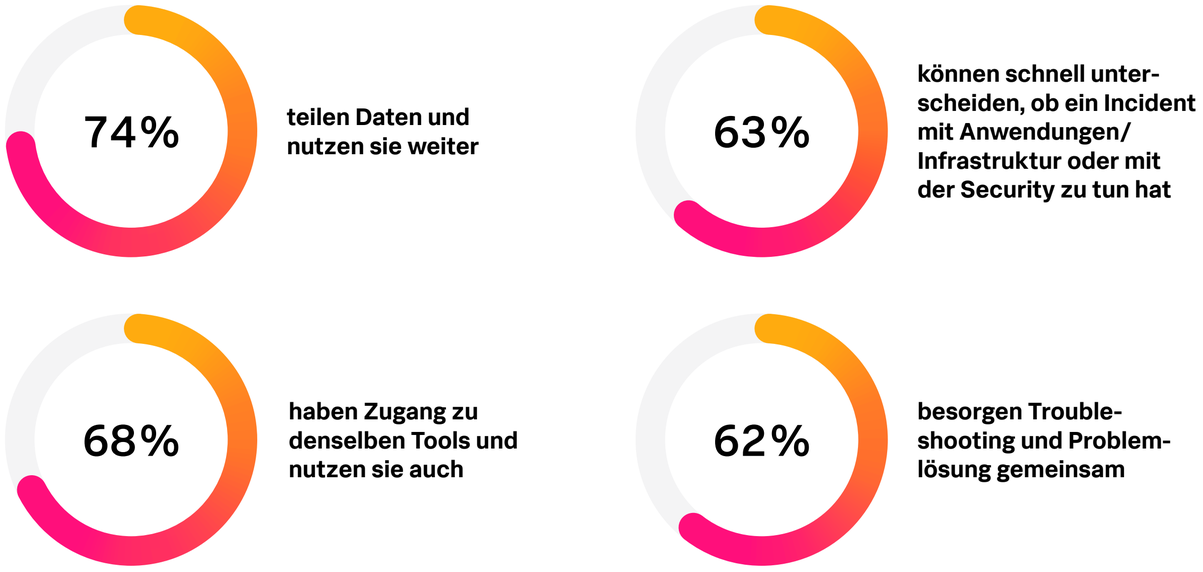
Daten hin und her zu reichen ist gut und schön, aber echte Teamarbeit findet erst dann statt, wenn die Observability- und die Sicherheitsteams von Anfang an gemeinsam an der virtuellen Front stehen und nicht erst darauf warten, dass einzelne Probleme nach und nach durch die getrennten Workflows sickern.

„Wenn die Software von Observability und Security isoliert arbeitet, kann es keine tiefen Beziehungen zwischen den Tools geben, und die Zusammenarbeit wird zu mühsamer Handarbeit“, sagt Mark Maslach, Vice President of Global Technical Sales Splunk Observability bei Cisco. „Das ist oft ein Zeichen für organisatorische Probleme.“

Weiter fortgeschrittene Formen der Zusammenarbeit zeigen den wahren organisatorischen Reifegrad, denn sie setzen voraus, dass die Teams ihre Silos aktiv aufbrechen und eng zusammenarbeiten. 62 % der Befragten sagen z. B., dass ihr Team das Troubleshooting und die Problemlösung gemeinsam mit dem Sicherheitsteam besorgt, und 63 % geben an, dass sie schnell unterscheiden können, ob Performance-Probleme bei Anwendungen und Infrastruktur Fehler-Ursachen haben, die in der Security liegen.

„Die Security-, ITOps- und Engineering-Teams werden wahrscheinlich immer bis zu einem gewissen Grad getrennt bleiben, weil ihre Skills und jeweiligen Motivationen einfach zu unterschiedlich sind“, sagt Craig Robin, Field CTO bei Splunk. „Es gibt jedoch Observability-Praktiken mit hohem Reifegrad, bei denen Incidents so schnell wie möglich priorisiert und dem entsprechend spezialisierten Team zugewiesen werden, wobei dafür gesorgt wird, dass das Team auch die richtigen Daten parat hat, die es braucht, um Probleme effizient zu lösen. Das ist die richtige Art und Weise, mit geschäftsrelevanten Problemen umzugehen.“

Die häufigsten Formen der Zusammenarbeit von Observability und Security



Qualifikationsdefizite und Silos erschweren die Zusammenarbeit

Die Zusammenarbeit von Observability- und Sicherheitsteams bei der Incident Response kann ein Zeichen für Observability-Praktiken auf hohem Reifegrad sein, aber so weit sind die meisten Teams noch nicht. Das größte Hindernis für eine bessere Zusammenarbeit mit der Security ist schlicht das Sträuben gegen Veränderungen – das sagen 59 % der Befragten.

Die Teams von Security und Observability haben bei Incidents grundverschiedene Ansätze. Die Sicherheitsteams legen ihren Nutzen als Menge der bearbeiteten Tickets dar („Wir haben 2000 potenzielle Angriffe gefunden und sie entschärft"). Dagegen sind die ITOps- und die Engineering-Teams bestrebt, die Anzahl der Incidents überhaupt gering zu halten. Möglicherweise zanken beide Parteien sogar, ob etwas überhaupt als Incident zu werten ist. Widerstand gibt es aber auch in Form von Schuldzuweisungen oder Schuldverschiebungen und im ewigen Streit um Zuständigkeiten.

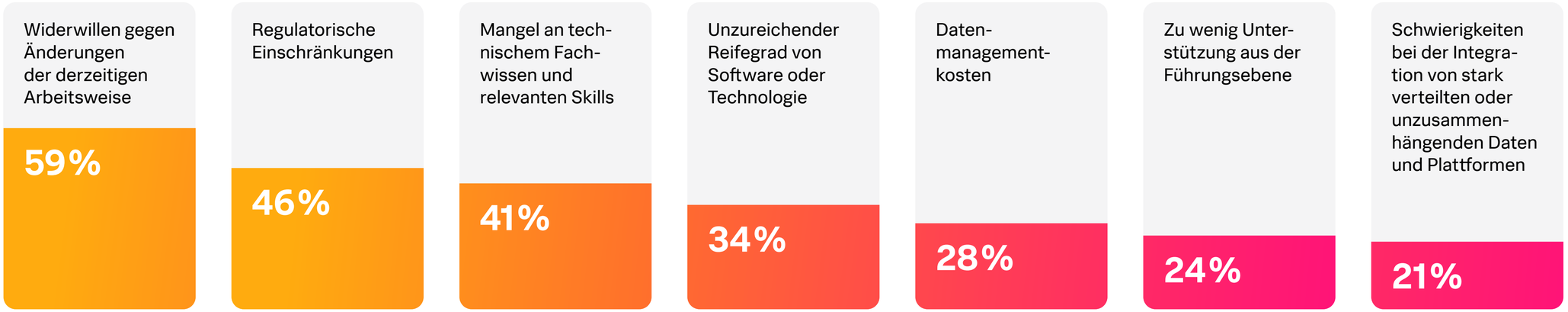
Wissenslücken sind ein weiterer Hauptgrund dafür, dass die Sicherheits- und die Observability-Teams nicht effektiv zusammenarbeiten. 41 % der ITOps- und der Engineering-Teams nennen den Mangel an technischem Fachwissen und an relevanten Skills als Herausforderung.

„SREs und NOC-Engineers haben nur wenig Ahnung, was Sicherheitsprobleme sind, weil sie dafür gar nicht ausgebildet sind", sagt Greg Leffler. „Die Security-Teams wiederum machen sich keine sonderlichen Sorgen um die Performance von Anwendungen, solange die Apps nicht gehackt werden."

Etwa ein Drittel der Befragten (34 %) nennt Software oder mangelnde technologische Reife als Hindernisse bei den Bemühungen um Zusammenarbeit. Viele Unternehmen arbeiten in der Tat immer noch mit separaten Plattformen für Sicherheit und für Observability, sodass es schwierig wird, Signale team- und systemübergreifend in Echtzeit zu korrelieren. Wenn z. B. die SIEM-Plattform (Security Incident and Event Management) eine DDoS-Warnmeldung für eine Kundenanwendung auslöst, zeigt die Observability-Software vielleicht nur die Performance-Probleme an, die dieser Angriff verursacht: höhere Latenzen, Fehlerraten, Ressourcenlast etc. Im Endeffekt stellt sich der Incident für die ITOps- und Engineering-Teams also als eine Reihe von Leistungsproblemen dar.

„Die am meisten fortgeschrittenen Unternehmen haben erkannt, dass Observability-Daten auch Security-Daten sind", sagt Craig Robin, „und sie verfolgen einen einheitlichen Ansatz, der es ermöglicht, dass Technologie die Knochenarbeit macht und die Sicherheitsauswirkungen identifiziert."

Die größten Hindernisse der Zusammenarbeit in der Praxis



Die Befragten konnten eine Mehrfachauswahl treffen.

Kapitel 4

Observability im KI-Zeitalter

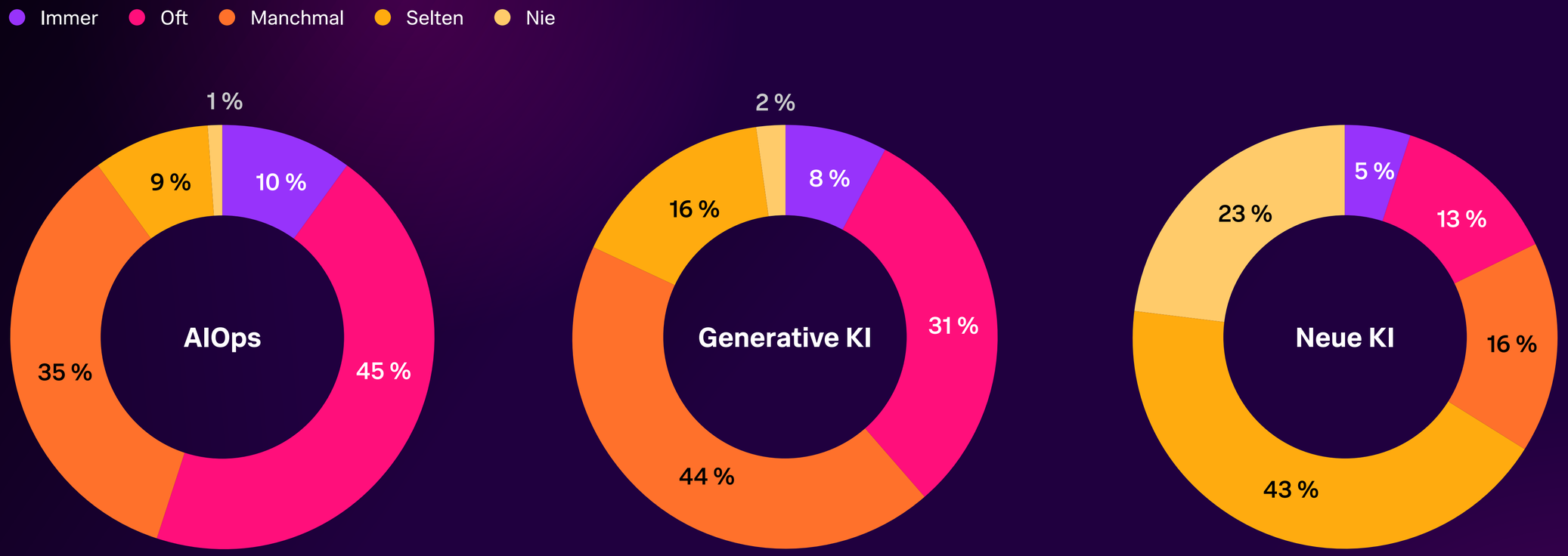
KI hat selbst die hartgesottenen Skeptiker neugierig gemacht, seit deutlich ist, dass sie bei richtiger Implementierung (mit Betonung auf „richtig“) einen unglaublichen Mehrwert bietet.

Der Großteil der Teams hat sich KI zu eigen gemacht: 76 % der Befragten nutzen KI regelmäßig in ihren täglichen Workflows. Allerdings hängen die Akzeptanzraten stark davon ab, um welche Art von KI es geht: 54 % arbeiten *oft* oder *immer* mit AIOps – einer ITOps-Komponente, die es nun seit fast einem Jahrzehnt gibt –, und 39 % nutzen *oft* oder *immer* generative KI.

Nur 18 % nutzen *oft* oder *immer* neue KI-Technologien wie autonom agierende KI (Agentic AI), eine Form von KI, die lernen, schlussfolgern, sich anpassen und vor allem autonom handeln kann, sodass sie ganze Workflows selbstständig übernehmen kann, etwa beim Programmieren und Debuggen von Software. Agentic AI wächst derzeit schnell, und es ist zu erwarten, dass der Einsatz in den nächsten Jahren heftig zunimmt.

Die Observability-Praxis greift zu KI

Wie oft die einzelnen KI-Formen im Einsatz sind



KI macht innovativ und beschleunigt die Fehlersuche

Den Teams ist durchaus bewusst, wie sehr KI die Produktivität steigern kann. 78 % sagen, dass sie dank KI mehr Zeit für Innovationen als für die Wartung aufwenden können, was zu besseren Geschäftsergebnissen führt. So können sich die Teams auf hochgradig effektive Vorhaben konzentrieren, die von der Implementierung von Microservices und Serverless-Technologien bis zur Entwicklung neuer digitaler Produkte reichen.

Dies dürfte Musik in den Ohren der Teams sein, die momentan noch Mühe haben, ihre Prioritäten umzusetzen. Immerhin 42 % geben aktuell zu, dass sie mehr Zeit als nötig für die Wartung ihrer Apps aufwenden. Fast die Hälfte der Befragten (45 %) hat weniger Zeit als nötig für die Entwicklung neuer Software übrig, wobei 12 % dieser Gruppe *deutlich* weniger Zeit als nötig haben – das ist der höchste Wert aller von uns abgefragten Aufgaben.

Generative-KI-Assistenten können helfen, indem sie z. B. Fragen zu Anwendungen und zur Infrastruktur beantworten, was besonders für weniger erfahrene Teammitglieder von Vorteil ist, die sich ansonsten komplett aufreiben würden. So können Junior Engineers z. B. bei einer Service-Unterbrechung die generative KI beauftragen, eine Trace-ID zu analysieren, und bekommen dann Empfehlungen zur Problemlösung und sogar einen kompletten Incident-Report.

„Geben Sie Ihren Junior-Analysten Tools an die Hand, die Logs, Metriken und Traces präzise analysieren können, und überlassen Sie der generativen KI die mühsame Arbeit der Kontext- und Mustererkennung“, sagt Cory Minton, Field CTO bei Splunk. „Dann können sich Ihre besten Leute im Engineering auf die Arbeit konzentrieren, die wirklich wichtig ist, z. B. auf Automatisierung oder die Entwicklung skalierbarer Engineering-Systeme.“

Die Befragten gehen davon aus, dass KI besonders in den Bereichen, die für das Geschäft am wichtigsten sind, von Nutzen sein wird. Als wichtige Observability-Fähigkeit wird am häufigsten die Erkennung von Schwachstellen und Bedrohungen bei Anwendungen genannt. 58 % der Befragten glauben, dass sich KI in diesem Bereich positiv auswirken wird.

Die Observability-Fähigkeiten von Troubleshooting und Fehler-Ursachen-Analyse halten 69 % für *einigermaßen wichtig* bis *sehr wichtig* für das Geschäft, und die Befragten gehen davon aus, dass KI hier am meisten helfen wird – ganze 60 % sagen, dass sie von KI in diesem Bereich eine positive Wirkung erwarten. Insbesondere AIOps kann die Fehler-Ursachen-Analyse beschleunigen, weil sich damit bei Service-Problemen granulare Trends entdecken und Probleme auf Code-Ebene identifizieren lassen.

Das rasante Wachstum generativer KI hat den Weg für autonom agierende KI geebnet, die noch komplexere Observability-Aufgaben selbstständig übernehmen kann. Wir bewegen uns auf eine Zukunft zu, in der KI-Agenten ganze Incident-Workflows von Anfang bis Ende managen können.

— Julie Gibbs, Vice President of Splunk AI and Integrations Product Marketing, Splunk

78 %

wenden dank KI mehr Zeit für Innovation auf als für die Wartung

KI setzt durchgängige Datenqualität voraus

KI einfach anzuschließen und auf ein Wunder zu warten, genügt nicht, wenn das Geschäft von den Vorteilen profitieren soll. Eine erfolgreiche KI-Einführung – oder auch nur KI-ready zu werden – setzt einiges mehr voraus, z. B. die Einbindung in die alltäglichen Abläufe der Teams, ein Verständnis der Funktionsweise und der Ergebnisse, eine Messung des Nutzens, eine nachhaltige Implementierung, bis das Unternehmen schließlich die Früchte erntet (oder nicht).

Wenn es um den KI-Erfolg geht, sind die Datenqualität und die Datenmengen gleichermaßen entscheidend. Geringe Datenqualität ist das Haupthindernis, wenn Unternehmen KI-ready werden wollen: 48 % der Befragten nennen dies als eine der größten Herausforderungen.

„In vielen Fällen gibt es niemanden, der ausdrücklich für die Datenqualität verantwortlich ist“, sagt Greg Leffler. „Stattdessen sagt ein Entwicklungs- oder SRE-Team: ‚Erfassen wir einfach die goldenen Signale – Latenz, Fehler, Traffic und Sättigung – mit diesen vier Metriken‘, und die Datenqualität muss nur gut genug sein, dass sie für das Troubleshooting ausreicht.“

Wer sollte also die Verantwortung übernehmen? Diejenigen, denen Observability am Herzen liegt, können ein praktisches Kompetenzzentrum bilden und Datenqualitätsstandards für das gesamte Unternehmen definieren und durchsetzen. Dazu gehört auch die Zusammenarbeit mit relevanten Interessengruppen wie dem Compliance-Team, damit sichergestellt bleibt, dass die Daten den Anforderungen aller gerecht werden.

Bereit für KI? Die größten Hindernisse

1. Mangelnde Datenqualität
2. Kosten der KI-Infrastruktur
3. Mangelndes Fachwissen oder Verständnis in den Teams
4. Widerwillen gegen Änderungen der derzeitigen Arbeitsweise
5. Unzureichende Datentransparenz

Die neue KI-Dynamik fordert die Observability-Teams

KI ist für Observability-Fachleute ein zweischneidiges Schwert. KI bewirkt, dass die Teams mehr schaffen, KI heißt aber auch, dass sie mehr Zeit für das Monitoring der neuen KI-Workloads aufwenden müssen. Fast die Hälfte der Befragten (47 %) klagt darüber, dass das Monitoring der KI-Workloads ihre Arbeit erschwert hat.

Dennoch ist die Fähigkeit, LLM-Daten zu verstehen und zu erfassen, von entscheidender Bedeutung, zumal die Relevanz von KI sich durch das gesamte Geschäft zieht.

KI-Workloads sind unglaublich dynamisch und ändern sich häufig, wenn die Modelle nachtrainiert oder aktualisiert werden. Außerdem können geringste Änderungen in den Daten – die sogenannte Data Drift – die Leistung des Modells beeinträchtigen, und zwar ohne dass dadurch Warnmeldungen ausgelöst werden.

KI hat auch keine typischen Workloads, sie hat eine ganz spezielle Infrastruktur, die oft außerhalb der typischen Anwendungsstapel situiert ist. Die Teams müssen bei KI-Workloads bestimmte Feinheiten beachten und erfassen, z. B. ob die GPUs am Limit sind. Und wie schnell werden Token generiert und verwendet? Wie ist die Reaktionszeit des Modells? Hat sich das Verhalten des Modells seit dem Nachtrainieren verändert? Und was am wichtigsten ist: Wie viel kostet das alles?

Dies sind Fragen, die ein ITOps- oder Engineering-Team möglicherweise nicht ohne Weiteres beantworten kann. Ein großes Hindernis sind dabei fehlende Fachkenntnisse bzw. mangelndes Verständnis: 40 % der Befragten nennen dies als große Herausforderung, wenn es darum geht, KI-ready zu werden.

„Es ist wichtig, dass ein einziges Team den gesamten Kontext hat, der zum Performance-Monitoring der gesamten Anwendung erforderlich ist, einschließlich der KI“, sagt Annette Sheppard, Director of Product Marketing for Observability bei Splunk. „Das bedeutet: Observability-Teams müssen ihre vorhandenen Fachkräfte weiterbilden und ihnen die Feinheiten beibringen, auf die sie achten müssen.“

47 %

sagen, dass das Monitoring von KI-Workloads die Arbeit erschwert hat

Wenn Ihre KI-Systeme nicht beobachtbar sind, sind sie ein Risiko. Wenn nämlich so ein Modell aus dem Ruder läuft, kann das schnell und manchmal unbemerkt geschehen. KI braucht Observability mehr als die meisten anderen digitalen Systeme, weil KI sich auf eine Art und Weise entwickelt, mit der Sie nicht rechnen.

— Cory Minton, Field CTO, Splunk

OpenTelemetry entwickelt sich vom Standard zur Strategie

In den vergangenen Jahren hat sich OpenTelemetry als Branchenstandard für die Erfassung von Observability-Daten in einem einheitlichen, leicht verständlichen Format etabliert. Praktisch jeder Observability-Anbieter (jedenfalls mehr als 40) unterstützt mittlerweile OpenTelemetry (OTel), und viele andere Anwendungen werden bereits mit integrierter Unterstützung ausgeliefert.

Die technischen Vorteile von OpenTelemetry sind hinlänglich bekannt. Der *Lagebericht Observability 2024: Wegbereiter für Erfolg* hat gezeigt, dass OpenTelemetry Unternehmen Zugang zu einem ausgedehnten Technologie-Ökosystem verschafft und es deutlich leichter macht, die Anforderungen an die Datenaufbewahrung zu erfüllen und moderne Cloud-Frameworks einzuführen. 2025 wird deutlich, dass die Vorteile weit über die Observability-Praxis hinausreichen. Bei der überwiegenden Mehrheit der Unternehmen, die OpenTelemetry zumindest gelegentlich nutzen, hat der Standard positive Auswirkungen auf das Umsatzwachstum (72 %), den operativen Gewinn (71 %) und die Markenwahrnehmung (71 %).

OTel-Power-User haben besseren Einblick

Wie kann es sein, dass OpenTelemetry eine solche Reichweite hat? OpenTelemetry erfasst mit relativ geringem Aufwand verteilte Traces, Metriken, Logs und Profile und reichert diese mit standardisierten Metadaten an, sodass sich Daten umgebungs-, sprach- und plattformübergreifend leicht vereinheitlichen lassen. Mit OpenTelemetry ist es ebenso einfach, zusätzlich benutzerdefinierte Daten zu erfassen, die relevante Business-Kennzahlen darstellen, oder die gesendeten Daten zu modifizieren. Mit derart umfangreichen Telemetriedaten können die Teams auch ganz spezielle Probleme lösen, die andernfalls unter dem Radar bleiben würden oder, noch schlimmer, erst dann bemerkt werden, wenn sich die Kundschaft beschwert.

Nehmen wir z. B. ein Unternehmen, das eine Website mit sehr starkem Traffic betreibt. Doch bei einem Teil der Besucher, die einen bestimmten Browser verwenden, gibt es Anmeldefehler. Ohne bestimmte Metadaten hätte das Unternehmen keinen Einblick in das Problem.

Die Vorteile von OpenTelemetry reichen über die Observability-Praxis hinaus

Wo sich OTel positiv auf das Geschäftsergebnis auswirkt

- **72%** Umsatzwachstum
- **71%** Operativer Gewinn
- **71%** Markenwahrnehmung
- **68%** Kundenzufriedenheit
- **67%** Innovationstempo

„Wenn die Teams OpenTelemetry einführen, bedeutet das in der Regel, dass sie einen Wendepunkt erreicht haben. Sie sammeln nicht nur Signale – sie investieren in Wissen, wie ihre Systeme tatsächlich funktionieren“, sagt Morgan McLean. „Dieser Bewusstseinswandel ist das, was einen hohen Reifegrad im modernen Engineering kennzeichnet.“

Je intensiver die Teams OpenTelemetry nutzen, desto mehr Vorteile ergeben sich. Die Befragten, die OTel stark nutzen – also oft oder immer – gehen mit Incidents ruhiger und systematischer um. Tatsächlich sagen hier 47 %, dass sie bei Incidents, die Kunden betreffen, *nie* in Panik geraten, während das diejenigen, die OpenTelemetry *selten* oder *nie* nutzen, nur zu 32 % von sich sagen können.

Die Power-User sagen auch dreimal häufiger als die OpenTelemetry-Nachzügler, dass ihre Observability-Praxis sich *deutlich* auf die Produktivität der Beschäftigten auswirkt. Auch eine *deutliche* Wirkung auf die Customer Experience wird von der Spitzengruppe doppelt so oft genannt wie bei den Nachzüglern.

OpenTelemetry-Anwender denken tendenziell auch bei anderen Technologien vorausschauender, vermutlich deshalb, weil sie eine Kultur geschaffen haben, die intellektuelle Neugier fördert und moderne Tools unterstützt. So arbeiten die OpenTelemetry-Power-User weit häufiger mit generativer KI, ChatOps, Observability as Code und automatisierter Fehlerbehebung. Die Mehrheit (57 %) der starken OpenTelemetry-Anwender nutzt z. B. *oft* oder *immer* Observability as Code – bei den Nachzüglern sind es nur 10 %.

Wenn Teams mit OpenTelemetry standardisieren, sammeln sie reichere Daten und legen die Grundlage für bessere Ergebnisse mit generativer KI. Denn eine einheitliche Telemetrie-Pipeline, kombiniert mit geschäftsbezogenen Tags wie der Kunden-ID und der jeweiligen Marketing-Kampagnengruppe, bedeutet reichhaltigere, konsistentere Daten für die KI-Modelle, was sich unmittelbar in kontextuellen Erkenntnissen, besseren Empfehlungen und weniger blinden Flecken niederschlägt.

OpenTelemetry ist die ultimative Grundlage jeder Observability-Lösung. Es ist der leistungsstärkste, am besten erweiterbare und zukunftssicherste Standard für Telemetrie.

— Morgan McLean, Senior Director of Product Management, Splunk, und Mitgründer von OpenTelemetry

OpenTelemetry-Power-User steigern Geschäftsergebnisse noch stärker

3×

höhere Produktivität der Mitarbeitenden

2×

mehr Wirkung auf die Customer Experience

Observability-Leader steigern Umsatz und ROI

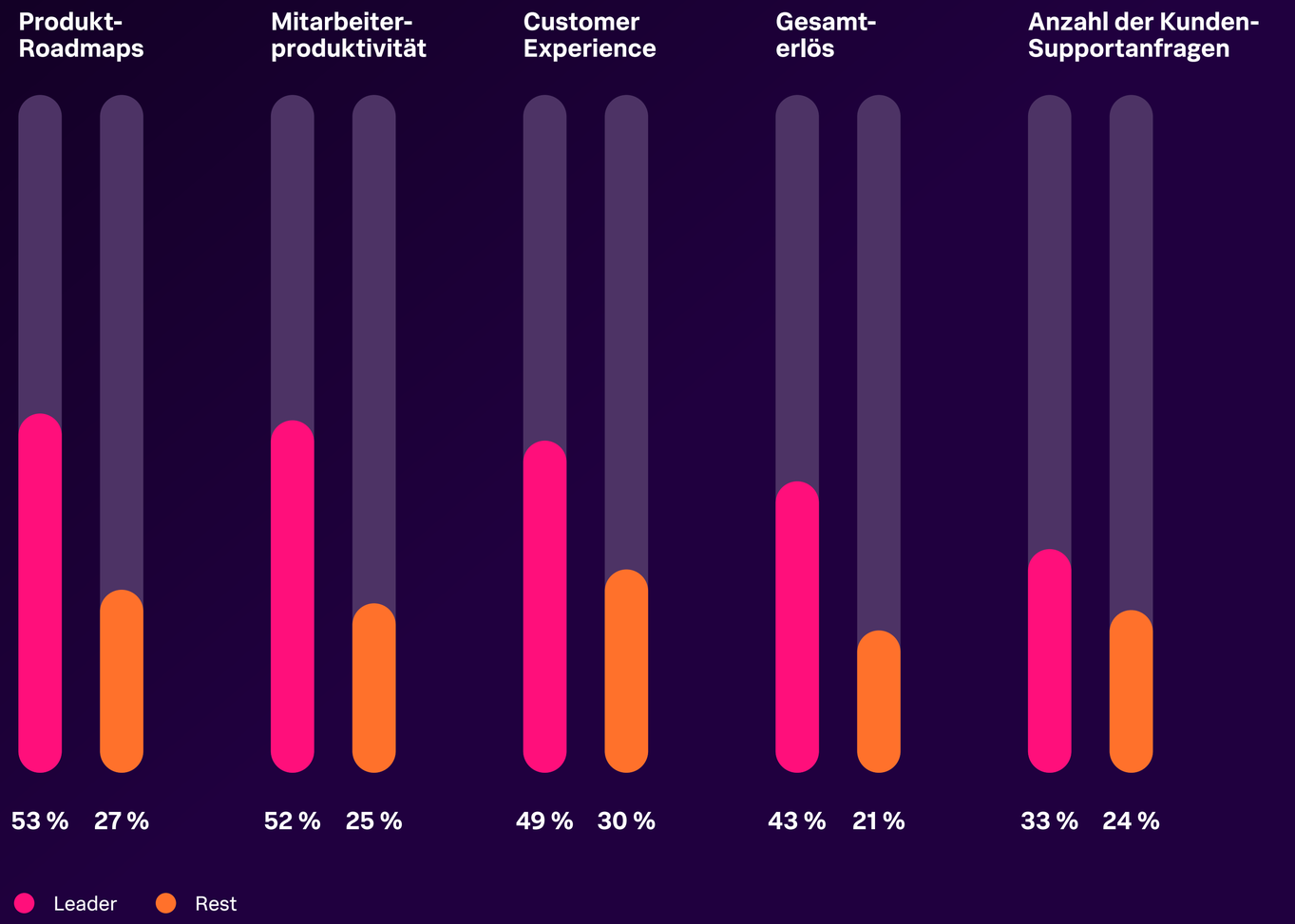
Bei Observability geht es nicht mehr nur darum, die Systeme irgendwie am Laufen zu halten. Observability prägt das Geschäft maßgeblich mit. Die Fachleute aus ITOps und Engineering haben heute Einfluss auf entscheidende Kennzahlen wie Umsatz und Customer Experience, und die wirkmächtigsten Teams fungieren als genuine Wachstumstreiber, die die Leistung des gesamten Unternehmens steigern.

Im Rahmen unserer Untersuchung haben wir eine Gruppe von Befragten identifiziert, die sich von den anderen dadurch abhebt, dass sie durchweg bessere Ergebnisse erzielt als der Rest. Diese Leader betreiben Observability auf dem Stand der Technik und dehnen ihren Einfluss auf das gesamte Unternehmen aus. So sagen sie z. B. doppelt so häufig wie der Rest, dass ihre Observability-Praxis den Gesamtumsatz, die Mitarbeiterproduktivität und die Produkt-Roadmaps *deutlich* verbessert. Sie erzielen außerdem einen jährlichen Observability-ROI von 125 % – das sind 53 % mehr als im übrigen Feld.

Was die Befragten der Leader-Gruppe gemeinsam haben, ist vor allem eine erstklassige technologische Grundlage; sie setzen *oft* oder *immer* zukunftsweisende Technologien ein, namentlich OpenTelemetry, Code-Profiling und Observability as Code.

Observability-Leader erweitern ihren Wirkungsbereich

Wo Observability-Praktiken *deutlich* positive Auswirkungen auf das Geschäft haben



Code-Profiling und Observability as Code führen zu besseren Ergebnissen

OpenTelemetry haben wir in Kapitel 5 ausführlich besprochen – angesichts von fast drei Vierteln (72 %), die sagen, dass OTel positive Auswirkungen auf das Umsatzwachstum hat, dürfte der Nutzen klar sein. Sehen wir uns nun Code-Profiling und Observability as Code genauer an.

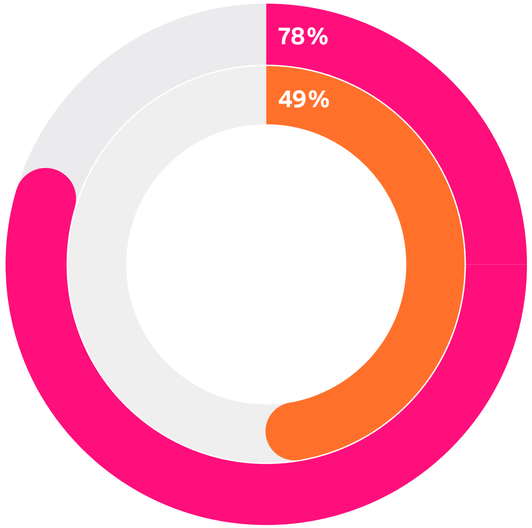
Code-Profiling erschließt eine weitere, noch detailliertere Ebene beim Troubleshooting, auf der die Teams problematischen Quellcode bzw. ganz präzise den konkreten Aufruf und die zugehörige Quellcodezeile identifizieren können. Sie wissen dann exakt, an wen aus dem Engineering sie sich wenden müssen und wie das Problem zu beheben ist. Beachtliche 78 % der Leader geben an, dass Code-Profiling hilft, Fehler-Ursachen schneller zu finden, und zwar *deutlich* oder gar *transformativ.*

Denn jede Minute Verzögerung bedeutet Kundenabwanderung und Umsatzeinbußen, daher ist Präzision das A und O.

„Wer keine Möglichkeit hat, Fehlerquellen genau zu lokalisieren, muss wie eine Feuerwehr arbeiten, die weiß, dass es irgendwo in der Gegend brennt, aber nicht, in welchem Haus“, sagt Greg Leffler. „Code-Profiling gibt Ihnen diese Klarheit – Sie können damit genau bestimmen, in welchem Haus, in welchem Stock und sogar in welchem Raum es brennt.“

Observability as Code wiederum ist ein DevOps-Ansatz, bei dem die Observability-Konfigurationen wie Code behandelt werden. Das bedeutet, dass die Teams Änderungen verfolgen, effektiv zusammenarbeiten und die Konfigurationen mithilfe von Versionskontrollsystemen z. B. zurücksetzen können. Außerdem können sie Dashboards, Warnmeldungen und andere Observability-Komponenten in derselben Sprache und mit denselben Methoden erstellen, die sie auch bei der Erstellung der Anwendungen verwenden. Das heißt, dass die Software-Engineering-Teams Observability als Grundbestandteil des Entwicklungsprozesses behandeln und nicht als nachträgliche Maßnahme. Aus all dem ergeben sich Konsistenz, Standardisierung und Skalierbarkeit.

„Observability as Code ist einer der deutlichsten Anzeiger einer Observability-Praxis von hohem Reifegrad“, sagt Patrick Lin. „Daran zeigt sich, dass Observability in den Entwicklungsprozess integriert ist und die Erfassung und Interpretation von Telemetriedaten mit der gleichen Disziplin behandelt wird wie der sonstige Code. Observability wird damit versioniert, automatisiert und konsistent.“



Leader finden mit Code-Profiling den schnellsten Weg zu den Fehler-Ursachen

Wo die höhere Geschwindigkeit *signifikant* oder *transformativ* ist

Leader Rest

Wer keine Möglichkeit hat, Fehlerquellen genau zu lokalisieren, muss wie eine Feuerwehr arbeiten, die weiß, dass es irgendwo in der Gegend brennt, aber nicht, in welchem Haus. Code-Profiling gibt Ihnen diese Klarheit – Sie können damit genau bestimmen, in welchem Haus, in welchem Stock und sogar in welchem Raum es brennt.

— Greg Leffler, Director of Developer Evangelism, Splunk

Für eine Kultur, die Business-orientiert ist

Die jeweilige Technologie – Code-Profiling, Observability as Code und OpenTelemetry – ist sicherlich hilfreich, doch es sollte klar sein, dass ihre Verwendung lediglich ein *Anzeichen* des Reifegrads ist und nicht der Grund. Es sind immer Menschen, die hinter der Entscheidung stehen, in zukunftsweisende Technologien zu investieren. Und diese Entscheidung steht für fortschrittliche Qualitäten wie das Interesse an Innovation, das Streben nach erstklassiger digitaler Experience, das konzertierte Bemühen um Teilhabe an der gesamten Observability-Landschaft und eine Beharrlichkeit im Lernen und in der Weiterbildung der eigenen Skills.

„Für mich zeigt das, dass es im Unternehmen Menschen gibt, denen die Kunst der Observability am Herzen liegt, und dass jemand die richtige Kultur dafür schaffen will“, sagt Craig Robin. „Das sind die Teams, die sich die Mühe machen, Observability zu einem Teil der kulturellen DNA des Unternehmens zu machen, die zu neuen Technologien greifen, die forschen und lernen, interne Teams anstoßen und ihre Investitionen in Zeit und Geld auch begründen können.“

Neben der Investition in Tools sollten wir uns noch genauer ansehen, wie Wachstumstreiber konkret zu besseren Geschäftsergebnissen führen.

Observability-Leader hängen den Rest des Feldes ab

Von Observability-Daten profitiert die Security

Die Observability-Leader arbeiten in den entscheidenden Bereichen tendenziell effektiver mit den Sicherheitsteams zusammen. Datenaustausch und Datenweiternutzung sind bei den Leadern weiter verbreitet (59 %) als bei den übrigen Befragten (45 %). Das dies ist nur der erste Schritt in der Zusammenarbeit. Fast die Hälfte (44 %) bestätigt *voll und ganz,* dass ihre ITOps- und Engineering-Teams Troubleshooting und Problemlösung gemeinsam mit den Security-Teams besorgen – beim Rest liegt der Anteil nur bei 29 %.

Diese Zusammenarbeit wird augenscheinlich durch die Tools erleichtert, auf die die Leader setzen. OpenTelemetry z. B. gibt den Observability- und den Sicherheitsteams eine gemeinsame Sprache zur Zusammenarbeit, sie arbeiten mit denselben Signalen und demselben Kontext. Entsprechend sagen nur 16 % der Leader, dass unausgereifte Software der Zusammenarbeit im Wege steht, während von den übrigen Befragten 35 % über hinderliche Toolsets klagen. Und lediglich 7 % der Leader berichten von Schwierigkeiten bei der Integration stark verteilter bzw. unverbundener IT-, Engineering- und Security-Plattformen – das sind dreimal weniger als beim Rest.

Vermutlich haben Telemetriedaten bei der Leader-Gruppe aufgrund der engeren Zusammenarbeit einen insgesamt größeren Nutzen für alle Teams. Bei den Sicherheitsteams der Leader-Gruppe spielt jede Art von Observability-Daten, die wir abgefragt haben – Metriken, Events, Traces und Logs – eine größere Rolle als bei den Sicherheitsteams der übrigen Befragten. Insbesondere Traces sind bei den Leadern 2,6-mal häufiger *deutlich* relevant für Sicherheitsentscheidungen als beim Rest des Feldes.

Dies ist ein handfester Beleg dafür, dass die Leader ihre Silos aufbrechen. Wenn die Sicherheitsteams aktiv Traces nutzen, bedeutet das, dass Daten nicht nur gemeinsam genutzt werden, sondern dass sie auch über das Engineering hinaus von den Teams verstanden und angenommen werden.

Observability-Leader erschließen KI-Vorteile

Kann es moderne Observability-Praktiken ohne KI geben? Wohl kaum. Während Observability-Leader auf der Welle der KI-Innovation reiten, paddelt der Rest noch mit den Händen. 64 % der Leader verwenden *oft* oder *immer* neue, aufkommende KI-Technologien wie autonom agierende KI – beim Rest sind es nur 15 %. Ähnliches gilt für generative KI und AIOps.

Den Leadern stehen auf ihrem dem Weg zu KI-Innovationen auch weniger Hindernisse im Weg. Speziell die Datenqualität ist weniger eine KI-Hürde: Nur etwa ein Drittel der Leader (34 %) nennt geringe Datenqualität als Herausforderung, bei den übrigen Befragten ist es fast die Hälfte (49 %). Auch die Wissenslücken sind weniger gravierend: Die Leader fühlen sich deutlich seltener auf ihrer KI-Reise durch fehlendes Fachwissen behindert (25 %) als der Rest (41 %).

Die Befragten der Leader-Gruppe sind auch der Überzeugung, dass KI wesentliche Abläufe verbessern wird. 42 % gehen davon aus, dass KI *deutlich* positive Auswirkungen auf das Monitoring kritischer Geschäftsprozesse haben wird; das übrige Feld ist dagegen weit weniger zuversichtlich (19 %).

Observability-Leader handhaben Warnmeldungen und Incidents präziser

Warnmeldungen sind bei den meisten Unternehmen ein Grund zur Besorgnis, doch längst nicht so sehr für die Gruppe der Observability-Leader. Beim Rest des Feldes klagt über die Hälfte (52 %) darüber, dass sich die Menge der Fehlalarme negativ auf die Teammoral auswirkt – bei den Leadern sind es fast 20 Prozentpunkte weniger (35 %).

Das dürfte auch daran liegen, dass Leader in der Regel eine bessere Warnmeldehygiene und bessere Incident-Response-Prozesse haben. 37 % sagen von sich, dass sie *nie* eine Warnmeldung verpassen, was bei den übrigen Befragten nur 15 % behaupten können. Und die Leader sagen 2,3-mal häufiger als der Rest, dass sie immer einen detaillierten Reaktionsplan entwickeln, wenn Incidents Folgen für die Kundschaft haben. Die Leader geben auch häufiger an (43 %) als der Rest (22 %), dass sie Incidents *oft* oder *immer* isolieren, an ein bestimmtes Team verweisen und darauf vertrauen, dass dieses Team das Problem löst – statt gleich mehrere Teams einzuschalten und unnötig Ressourcen zu verbrennen.

Ihr Weg zum Wachstumstreiber

Observability-Praktiken auf der Höhe der Zeit wirken als Wachstumstreiber, der höhere Umsätze, eine bessere Customer Experience und noch eine ganze Menge weiterer relevanter Ergebnisse auswirft. Der Nutzen von Observability-Anwendungsdaten zieht sich durch das gesamte Geschäft und ist keineswegs auf die Observability-Ziele beschränkt.

Hier einige Ratschläge mit Blick auf die Ergebnisse der Befragung – wie Sie mit Ihren Observability-Praktiken für Business-Ergebnisse sorgen.

1 Halten Sie Krisenstäbe und Reaktionsaufwand in Grenzen

Panik ist selten gut. Gleichwohl müssen 21 % eingestehen, dass sie im Ernstfall *manchmal, oft* oder *immer* in Panik verfallen. Und 20 % geben an, dass sie *oft* oder *immer* einen Krisenstab einrichten, in dem zahlreiche Teams vertreten sind. Das bedeutet: Bis das Problem gelöst ist, werden Ressourcen verbrannt und die Produktivität geht gegen null.

- **Grenzen Sie den Incident auf ein bestimmtes Team ein.** Wenn Sie schnell feststellen können, ob ein Problem mehr die Security oder die Observability betrifft, müssen sich die Teams nicht doppelt auf die Suche machen. Im Idealfall geschieht das Troubleshooting durch ITOps, Engineering und Security Hand in Hand, alle tauschen Kontext und Erkenntnisse aus, ermitteln die Fehler-Ursache und weisen den Incident dann dem passenden Team zu.
- **Machen Sie routinemäßig Post-mortem-Analysen.** Die Teams lernen dann aus vergangenen Erfolgen und Fehlern und sind nicht dazu verdammt, die Geschichte zu wiederholen. Verankern Sie Post-mortem-Untersuchungen als Standard im Incident-Response-Prozess und stellen Sie sicher, dass die Analysen als lebende Dokumente behandelt werden, sodass spätere Änderungen an Richtlinien, Tools oder Plänen berücksichtigt werden.

2 Gewinnen Sie Kontrolle über Warnmeldungen

Eine der Hauptstressquellen für ITOps- und Engineering-Teams sind Fehlalarme. 54 % der Befragten geben an, dass ihr Observability-ROI am meisten von der Qualität der Warnmeldungen abhängt. Die Warnmeldungen in den Griff zu kriegen, lohnt sich also.

- **Optimieren Sie das Feintuning mit adaptiver Schwellenwertberechnung.** Orientieren Sie Ihre Schwellenwerte an der Kritikalität des zu überwachenden Systems bzw. Services, filtern Sie verrauschte falsch Positive aus und stellen Sie sicher, dass jede Warnmeldung valide ist. Mit adaptiven Schwellenwerten können Sie die Normalwerte dann auf der Basis historischer Daten dynamisch anpassen.
- **Unterdrücken Sie Warnmeldungen nur aus *wirklich* gutem Grund.** Die Warnmelde-Unterdrückung sollten Sie, wenn überhaupt, nur extrem sparsam verwenden; am besten lassen Sie das Ihr CD-System (Continuous Deployment) für Sie erledigen. Die Entscheidung darüber sollten Sie wohlüberlegt treffen und am besten mit einem ganz konkreten Grund unterfangen – das könnte z. B. ein anstehendes Roll-out oder eine planmäßige Wartung sein, aber sicher nicht unvermutete Traffic-Spitzen.

3 Machen Sie Ihre Daten durch Qualitätsstandards KI-tauglich

Beachtliche 78 % der Befragten sagen, dass sie durch KI mehr Zeit auf Innovationen als auf die Wartung verwenden; dennoch notieren 48 % – also fast die Hälfte –, dass mangelnde Datenqualität sie daran hindert, sich KI-ready aufzustellen.

- **Klären Sie die Verantwortung für die Datenqualität.** In vielen Unternehmen sind die Zuständigkeiten für die Qualität der Anwendungstelemetrie unklar. Oft wird die Verantwortung wie selbstverständlich dem Platform Engineering zugeschoben, unabhängig davon, ob das Team die Kapazitäten und das Fachwissen dafür hat. Also: Bilden Sie eine Gruppe von Leuten, die sich für Observability begeistern, und geben Sie dieser Gruppe die Befugnis, Datenqualitätsstandards aufzusetzen und durchzusetzen, die dann unternehmensweit Geltung haben. Beziehen Sie Interessengruppen wie das Compliance-Team mit ein, sodass die Anforderungen aller Seiten erfüllt werden. Wenn Sie deutlich machen, dass eine bessere Datenqualität interessante neue Fähigkeiten möglich macht, wird das die Bereitschaft der Teams, mitzuwirken, deutlich verbessern.
- **Ergänzen Sie Business-Kontext und Tags.** Die Erkenntnisse, die Ihre KI (und Ihre Leute aus dem Engineering) gewinnen, können Sie gut anreichern, indem Sie Tags mit relevanten Business-Informationen nutzen. Das könnte z. B. die Anwendung sein, von der das Problem ausgeht, die Versionsnummer, die Umgebung oder der angemeldete User. Mit diesem zusätzlichen Kontext können Ihre Teams Muster entdecken, die mit den geschäftlichen Auswirkungen korrelieren – etwa ob das Problem VIP-Kunden betrifft –, und ihre Warnmeldungen und Reaktionen entsprechend priorisieren.

4 Wagen Sie sich an zukunftsweisende Technologien

Eine Gruppe, die wir „Business-Katalysatoren“ nennen, gibt doppelt so häufig an wie der Rest, dass ihre Observability-Praxis den Gesamterlös deutlich verbessert. Was haben diese Befragten gemeinsam? In erster Linie das Engagement für zukunftsweisende Technologien – sie arbeiten oft oder immer mit OpenTelemetry, Code-Profiling und Observability as Code.

- **Beginnen Sie mit dem größten Engpass.** Alle drei Technologien gleichzeitig einzuführen, wäre ein gewagtes Unterfangen. Ermitteln Sie Ihre Prioritäten und entscheiden Sie von dort aus. Falls Ihre Observability-Praktiken zu langsam in der Problemerkennung sind, dann könnte Code-Profiling ein guter Anfang sein. Falls Ihr Team sich schwertut, Daten in einheitlichem Format zu erfassen, dann ist OpenTelemetry der richtige erste Schritt.
- **Sorgen Sie für Wissensaustausch.** Wenn die Observability-Vorreiter im eigenen Haus Gelegenheit hatten, sich weiterzubilden, sollten Sie monatlich oder vierteljährlich, in jedem Fall aber regelmäßig technische Sessions veranstalten, auf denen die Spitzenkräfte mit dem übrigen Team über aktuelle Entwicklungen bei Observability-Tools, über neue Frameworks und sonstige Fortschritte sprechen können. In diesen Foren können auch neue Tools diskutiert und Schwierigkeiten bei der Implementierung angesprochen werden. All das trägt zu einer breiteren Akzeptanz bei.

Ihre nächsten Stopps Richtung Observability-Leadership

Digitale Resilienz – Der Podcast von Leadern, für Leader

Neugierig auf noch mehr Observability-Trends? Finden Sie heraus, wie Führungskräfte die anstehenden Herausforderungen von heute angehen: KI, Datenmanagement und Innovationen für Entwickler.

Mehr erfahren

Die neuen Regeln des Datenmanagements

Finden Sie heraus, wie Sie Datenvolumen und -komplexität in den Griff bekommen. Mit den neuen Regeln des Datenmanagements machen Sie Cybersicherheit und Observability noch effektiver.

Bericht lesen

Branchen-Highlights

Wir haben für Sie die wichtigsten Erkenntnisse aus vier ausgewählten Branchen zusammengestellt.

Finanzdienstleister

Bei den Unternehmen aus dem Finanzsektor hängen Observability und Business eng zusammen. Mehr als drei Viertel (77 %) geben an, dass sich ihre Observability-Praktiken positiv auf den Umsatz auswirken – ein Wert, der deutlich über dem Durchschnitt von 65 % liegt. Und 75 % sagen, dass Observability ihre Produkt-Roadmaps mitbestimmt. Dies entspricht auch den Prioritäten bei den Observability-Funktionen: Für 40 % ist das Monitoring kritischer Geschäftsprozesse *sehr* wichtig für das Gesamtgeschäft.

Insgesamt ist die Branche ausgesprochen KI-affin, 46 % äußern sich optimistisch zu den Potenzialen von KI – der Vergleichswert des Gesamtdurchschnitts liegt nur bei 36 %. Doch die Finanzdienstleister sehen auch die Herausforderungen deutlicher, die KI mit sich bringt. Während im Gesamtdurchschnitt 47 % sagen, dass das Monitoring von KI-Workloads die Arbeit erschwert hat, ist es im Finanzsektor über die Hälfte (54 %).

Was die Tools betrifft, ist OpenTelemetry bei den Finanzdienstleistern relativ weit verbreitet. 36 % sagen, dass sie OTel *oft* oder *immer* verwenden (Vergleichswert: 26 %). Und sie profitieren davon auch häufiger: Drei Viertel (75 %) der Unternehmen, die OpenTelemetry zumindest gelegentlich nutzen, geben an, dass sich die Technologie positiv auf den Erlös ausgewirkt hat.

Eine echte Zusammenarbeit zwischen den Observability-Teams und den Security-Teams ist in der Branche allerdings weniger häufig. Dass ITOps-, Engineering- und Sicherheitsteams dieselben Tools verwenden, kommt hier seltener vor (59 %) als im Gesamtdurchschnitt (68 %); auch der teamübergreifende Austausch von Daten geschieht im Finanzsektor seltener (61 %) als im Vergleichsdurchschnitt (74 %). Als größtes Hindernis werden die regulatorischen Vorgaben genannt (60 %) – das ist bei einer Branche, in der Compliance ein entscheidender Faktor ist, nur verständlich.

Die Abschottung der Teams dürfte auch ein Grund dafür sein, dass die Teams der Finanzdienstleister bei Incidents unter großem Druck stehen. 12 % geben an, dass bei kundenrelevanten Events *oft* oder *immer* Panik herrscht – das ist spürbar mehr als im Gesamtdurchschnitt (9 %).

Action Guide für den Finanzsektor lesen.

Fertigung

Auch in den Fertigungsunternehmen haben die Observability-Praktiken starke Auswirkungen auf das Geschäft, insbesondere auf die Produktivität der Beschäftigten. In diesem Punkt geben die Befragten der Branche öfter (86 %) als der Gesamtdurchschnitt (74 %) eine Verbesserung zu Protokoll.

Die Zusammenarbeit der ITOps-, Engineering- und Security-Teams ist in den produzierenden Unternehmen deutlich besser als im Durchschnitt. 97 % in der Branche arbeiten mit gemeinsamen Daten und nutzen sie auch weiter, 81 % besorgen Troubleshooting und Problemlösung gemeinsam mit den Sicherheitsteams.

In der Observability-Praxis der Fertigung spielt KI eine wichtige Rolle. Fast die Hälfte (48 %) zeigt sich in Bezug auf die Vorteile von KI für ihre Teams sehr optimistisch. Hinzu kommt, dass die Befragten deutlich weniger Probleme haben, sich KI-ready aufzustellen. Namentlich die mangelnde Datenqualität ist in der Fertigung seltener (35 %) ein Hindernis als im Gesamtdurchschnitt der Branchen (48 %).

Die Fertiger sind nicht nur optimistisch, was KI angeht, sondern nutzen KI in ihren fortschrittlichsten Formen. Beachtliche 45 % der Befragten geben an, dass sie neue KI-Formen *oft* oder *immer* nutzen – der Vergleichswert liegt bei nur 18 %. Und fast alle Befragten (94 %) sagen, dass sie dank KI weniger Zeit für die Wartung aufwenden müssen und stattdessen mehr Zeit für Innovationen haben. Offenbar geht diese Zeit in die Software-Entwicklung, denn nur 39 % der Befragten aus produzierenden Unternehmen klagen darüber, dass sie zu wenig Zeit für die Entwicklung neuer Software haben; im Gesamtdurchschnitt ist dieser Mangel bei 45 % fühlbar.

Die Teams der Fertigung setzen auf fortschrittliche Observability-Tools und sind führend bei der Einführung einer ganzen Reihe von Technologien: Sie arbeiten *oft* oder *immer* mit automatisierten Abhilfemaßnahmen (43 %), Code-Profiling (41 %) und Observability as Code (39 %). Diese Investitionen, verbunden mit einem hohen Reifegrad in den Bereichen Zusammenarbeit und KI, positionieren die Fertigungsbranche als zukunftsorientierten Observability-Leader.

Action Guide für die Fertigung lesen.

Öffentliche Hand

Einrichtungen des öffentlichen Sektors sind derzeit erst noch dabei, herauszufinden, wie Observability ihren jeweiligen Zwecken möglichst unmittelbar dienen kann. Im Vergleich zu anderen Branchen geben die Befragten der öffentlichen Hand folglich deutlich seltener an, dass ihre Observability-Praxis eine positive Wirkung hat. Das gilt konkret etwa für Budget (30 % gegenüber 65 %), Produkt-Roadmaps (30 % gegenüber 64 %) und Mitarbeiterproduktivität (36 % gegenüber 74 %).

Für die Befragten der öffentlichen Hand hängt der ROI am engsten mit der betrieblichen Effizienz zusammen, insbesondere mit den Warnmeldungen: 69 % nennen die Qualität der Warnmeldungen als einen der wichtigsten ROI-Faktoren, womit der öffentliche Sektor noch einmal deutlich über dem ohnehin hohen Gesamtdurchschnitt von 54 % liegt. Dies deckt sich damit, dass die Teams der öffentlichen Hand als Hauptursache von Stress zu 61 % die hohe Anzahl von Fehlalarmen nennen.

Eindeutig ausbaufähig ist die Zusammenarbeit, ein für Ämter, Behörden und andere Organisationen des öffentlichen Sektors ohnehin schwieriges Thema. Nur 46 % der Teams im öffentlichen Sektor sagen, dass sie Observability-Daten teilen und weiternutzen, und nur bei 35 % geschieht das Troubleshooting teamübergreifend mit der Security – das ist der niedrigste Wert aller Branchen. Hinzu kommen weitere Hindernisse, speziell der Mangel an einschlägigen Skills (62 %) und ein niedriger Reifegrad der Technologie (60 %). In beiden Punkten liegt die öffentliche Hand deutlich über dem allgemeinen Branchendurchschnitt.

Observability im öffentlichen Sektor befindet sich derzeit erst noch im Auf- und Ausbau, insofern ist es logisch, dass die Branche kaum in der Lage ist, die Vorteile zukunftsweisender Technologien zu nutzen. Nur 35 % verwenden AIOps *oft* oder *immer* (Vergleichswert des Gesamtdurchschnitts: 54 %), nur 10 % setzen generative KI *oft* oder *immer* ein (Vergleichswert: 39 %) und nur 8 % nutzen Observability as Code *oft* oder *immer* (Vergleichswert: 29 %). Ähnlich heftig ist die Differenz bei Code-Profiling (2 % gegenüber 21 %) und OpenTelemetry (2 % gegenüber 26 %).

Action Guide für die öffentliche Hand lesen.

Kommunikation und Medien

Die Unternehmen aus der Kommunikations- und Medienbranche gehören in Sachen Observability zu den fortschrittlichsten – und ihr Geschäft profitiert entsprechend kräftig von den Vorteilen. Beachtliche 88 % geben zu Protokoll, dass sich ihre Observability-Praxis positiv auf den Gesamtumsatz auswirkt – der Durchschnittswert aller Branchen bleibt mit 65 % deutlich darunter. Und 81 % sagen, dass Observability sich positiv auf ihre Produkt-Roadmap auswirkt (Vergleichswert: 64 %).

Geschwindigkeit ist für diesen Sektor von größter Bedeutung. Für die meisten Befragten aus Kommunikation und Medien (68 %) ist daher die Troubleshooting-Geschwindigkeit im Fall eines Incidents der größte ROI-Faktor ihrer Observability-Lösungen. Im Gesamtdurchschnitt spielt das Tempo der Fehlersuche nur bei 49 % eine derart wichtige Rolle. Kommunikation und Medien messen auch KI große Bedeutung bei: 51 % geben an, dass ihr Observability-ROI in erster Linie vom Reifegrad ihrer KI-Funktionen abhängt.

Dass die Teams der Kommunikations- und Medienunternehmen im KI-Einsatz führend sind, sollte daher nicht überraschen. 79 % setzen oft oder immer KI ein, 68 % nutzen *oft* oder *immer* generative KI – beide Werte liegen weit über dem Durchschnitt. Eine Hürde sind jedoch weiterhin die Daten: 56 % nennen die Datenqualität als KI-Hindernis, 69 % nennen Datenherausforderungen wie Zugänglichkeit, Qualität und Fragmentierung als ihre größten Stressfaktoren.

Trotzdem gelingt es den Teams dieser Branche, bei der Sache zu bleiben. Sie klagen seltener (27 %) als der Gesamtdurchschnitt 43 %) darüber, dass sie zu viel Zeit mit der Bearbeitung von Warnmeldungen verbringen, und 73 % verpassen *selten* oder *nie* eine Warnmeldung, womit sie gut über dem Durchschnitt von 60 % liegen. Dennoch sagen 69 %, dass sie weniger Zeit für die Entwicklung neuer Software aufwenden, als ihnen lieb ist, was darauf hindeutet, dass es weiterhin konkurrierende Prioritäten gibt.

Die Unternehmen der Kommunikations- und Medienbranche sind auch Pioniere der OpenTelemetry-Einführung. 67 % nutzen OpenTelemetry oft oder immer – mehr als doppelt so viel wie im Durchschnitt aller Branchen. Und das zahlt sich aus: 86 % geben an, dass OpenTelemetry zur Erlössteigerung beiträgt, und 83 % verzeichnen eine positive Wirkung auf die Kundenzufriedenheit.

Action Guide für Kommunikation und Medien lesen.

Länder-Highlights

Schnappschüsse von neun ausgewählten Ländern auf der ganzen Welt.

Australien

Australien ist sowohl beim KI-Einsatz als auch bei fortschrittlichen Observability-Praktiken führend, und es gibt deutliche Anzeichen dafür, dass diese Investitionen messbare Geschäftsvorteile bringen. 45 % der Befragten geben an, dass sie von den Vorteilen, die KI ihren Teams bringen kann, begeistert sind – deutlich mehr als im weltweiten Durchschnitt (36 %). Diesem Optimismus folgen auch Taten: Die KI-Einführungsrate ist in allen drei KI-Kategorien höher, selbst neue Formen (wie autonom agierende KI) nutzt Australien zu 21 % *oft* oder *immer* – der Vergleichsdurchschnitt kommt nur auf 18 %.

Diese Voraussicht zahlt sich aus. 87 % sagen, dass sie dank KI mehr Zeit auf Innovationen verwenden statt auf die Wartung (Vergleichswert: 78 %). Dies könnte erklären, warum die Befragten seltener (37 %) als der Länderdurchschnitt (45 %) darüber klagen, dass sie weniger Zeit für die Entwicklung neuer Software übrig haben, als ihnen lieb ist. Dies könnte bedeuten, dass das Engineering down under sich Freiraum für wertschöpfende Arbeit verschafft hat. Dazu passt auch, dass die australischen Befragten höhere Erwartungen haben, wenn es darum geht, wie sich KI auf die Observability auswirkt. 72 % nehmen an, dass KI das Troubleshooting und die Fehler-Ursachen-Analyse verbessern wird – 12 % mehr als im Durchschnitt.

Australische Unternehmen nutzen auch OpenTelemetry in höherem Maße, es gibt hier mehr Befragte (36 %), die OTel oft oder immer einsetzen, als im Länderdurchschnitt (26 %). Entscheidend ist aber, dass sich der Einsatz auch zählbar im Geschäftsergebnis niederschlägt: 79 % der australischen Unternehmen, die OpenTelemetry zumindest manchmal nutzen, verzeichnen eine positive Wirkung auf die Erlöse. Damit liegen sie über dem Gesamtdurchschnitt von 71 %.

Deutschland

Die Observability-Praktiken in Deutschland schlagen sich in guten Geschäftsergebnissen nieder: 74 % der Befragten berichten von einer positiven Auswirkung auf den Gesamtumsatz – also deutlich mehr als im weltweiten Durchschnitt, der bei 65 % liegt. In dieser Leistung bildet sich nicht nur der technische Reifegrad ab, sondern auch ein auf Zusammenarbeit ausgerichteter Ansatz bei der Problemlösung, der die Teams enger zusammenbringt: 62 % der Befragten aus Deutschland sagen, dass Troubleshooting und Problemlösung von Observability- und Security-Teams gemeinsam besorgt werden.

Die Praxis der Incident-Reaktion zeigt allerdings ein komplexeres Bild. Einerseits führen 74 % der deutschen Teams *oft* oder *immer* ausführliche Post-mortem-Analysen im Nachgang von Incidents durch – etwas mehr als die 71 % des weltweiten Durchschnitts –, was ein Bemühen um kontinuierliches Lernen und um Verbesserung beweist. Andererseits geben 28 % an, dass sie bei Incidents, die Folgen für die Kundschaft haben, *oft* oder *immer* einen Krisenstab einrichten – und damit liegen sie klar über dem weltweiten Durchschnitt von 20 %.

In jedem Fall sind die deutschen Teams OpenTelemetry-Vorreiter: 32 % setzen OpenTelemetry *oft* oder *immer* ein. Und sie profitieren auch davon. 79 % derjenigen, die OpenTelemetry zumindest manchmal nutzen, sagen, dass sich das positiv auf den Erlös auswirkt; der weltweite Vergleichsdurchschnitt liegt bei 72 %.

Frankreich

Frankreich hat mit Datenherausforderungen zu kämpfen, die bei der KI-Einführung hinderlich und eine ständige Ursache von Stress für die Observability-Teams sind. 58 % nennen Datenprobleme, z. B. Zugänglichkeit und Qualität, als einen Hauptstressfaktor. Es überrascht daher nicht, dass 51 % der Befragten mangelnde Datenqualität auch als größtes Hindernis der KI-Einführung nennen.

Trotz dieser Hürden sind französische Unternehmen um operative Disziplin bemüht, insbesondere beim Management der Warnmeldungen und bei der Incident Response. Dass Warnmeldungen *oft* oder *immer* übersehen werden, kommt seltener vor (8 %) als im weltweiten Durchschnitt (13 %), was auf gute Warnmeldehygiene schließen lässt. Dies dürfte auch ein Grund dafür sein, dass es in Frankreich weniger Incident-Stress gibt. Lediglich 4 % sagen, dass sie bei Incidents, die Auswirkungen auf die Kundschaft haben, *oft* oder *immer* in Panik geraten. Der Länderdurchschnitt liegt bei 9 %.

Hinzu kommt, dass französische Unternehmen einen Schwerpunkt auf schnelle Incident-Behebung legen. 25 % sagen, dass der Observability-ROI am meisten von der Geschwindigkeit beim Troubleshooting von Incidents abhängt – eine schnelle, effektive Reaktion gehört in Frankreich also zu den Top-Prioritäten.

Für Geschwindigkeit sorgen sollen u. a. zukunftsweisende Tools, die in Frankreich relativ eifrig aufgegriffen werden. Das gilt namentlich für Code-Profiling, das mehr Befragte (30 %) *oft* oder *immer* einsetzen als im Länderdurchschnitt (21 %.) Deutlich ist auch, dass diese Investitionen strategisch sind. 43 % derjenigen, die Code-Profiling zumindest manchmal einsetzen, sind der Überzeugung, dass sie damit ihre KI-Fähigkeiten effektiver machen.

Indien

Die Teams in Indien arbeiten in hohem Maß mit den Security-Teams zusammen: 81 % sagen, dass sie Daten mit den Sicherheitsteams austauschen und nachnutzen; im weltweiten Durchschnitt sind es nur 74 %. Noch wichtiger ist, dass deutlich mehr (74 %) als im Gesamtdurchschnitt (65 %) bei Problemen mit der Performance von Anwendungen und Infrastruktur die Security-Ursachen genau bestimmen können. Dies legt nahe, dass es sich nicht nur um eine oberflächliche Zusammenarbeit handelt, sondern um eine echte technische Abstimmung zwischen den Funktionsbereichen.

Die Zusammenarbeit bringt aber auch Herausforderungen. Mehr als die Hälfte der Befragten in Indien (53 %) nennt regulatorische Beschränkungen als Haupthindernis einer verbesserten Zusammenarbeit.

Die KI-Nutzung ist ein weiterer Lichtblick. In Indien sagen 82 %, dass sie dank KI mehr Zeit für Innovationen statt für die Wartung aufwenden – sie liegen damit über dem weltweiten Durchschnitt von 78 %. Und deutlich weniger Befragte (36 %) als im weltweiten Vergleich (43 %) geben an, dass sie mehr Zeit als nötig mit der Bearbeitung von Warnmeldungen verbringen. Das könnte daran liegen, dass KI bereits einen Teil der operativen Last übernimmt.

Warnmeldungen spielen eine wesentliche Rolle bei der Gestaltung der Security-Strategie. 58 % der Befragten in Indien sagen, dass Warnmeldungen einen deutlichen Einfluss auf Sicherheitsentscheidungen haben (Vergleichswert: 47 %). Darüber hinaus geben 62 % an, dass der Observability-ROI maßgeblich von der Qualität der Warnmelde-Erkennungen abhängt. Es gibt aber auch einen Wermutstropfen: 55 % klagen darüber, dass sich die Menge der Fehlalarme negativ auf die Moral des Teams auswirkt.

Japan

In Japan verfolgt in der Observability-Praxis gegenüber neuen Zukunftstechnologien, insbesondere KI, einen Ansatz, der als vorsichtig, aber optimistisch zu bezeichnen ist. Bei der KI-Nutzung liegt das Land leicht unter dem Durchschnitt: Weniger Befragte (48 %) als im weltweiten Mittel (54 %) sagen, dass sie *oft* oder *immer* mit AIOps arbeiten, und nur 9 % geben an, dass sie *oft* oder *immer* neue KI-Formen wie autonom agierende KI nutzen. Der globale Vergleichswert liegt hier doppelt so hoch, bei 18 %.

Die größte Herausforderung, die einer breiteren KI-Nutzung im Wege steht, scheint die Datenqualität zu sein, die 47 % der Befragten aus Japan als Haupthindernis nennen. Darüber hinaus finden 53 %, dass das Monitoring von KI-Workloads ihre Arbeit erschwert – im Gesamtdurchschnitt liegt dieser Wert bei 47 %. Trotz dieser Hürden ist sich Japan offenbar bewusst, welches Potenzial in KI steckt. 62 % sind der Überzeugung, dass sich KI positiv auf das Monitoring kritischer Geschäftsprozesse auswirken wird, womit sie leicht über dem globalen Durchschnitt liegen.

Der Wildwuchs an Tools ist ein weiteres großes Problem, mit dem die Observability-Teams in Japan konfrontiert sind. 65 % der Befragten klagen darüber, dass die Vielzahl unverbundener Tools auf die Moral der Teams schlägt – dieser Motivationsdämpfer ist der am häufigsten genannte, Japan liegt damit zehn Prozentpunkte über dem weltweiten Durchschnitt (59 %). Die Tool-Fragmentierung kann auch zu Alarmmüdigkeit und Transparenzlücken führen. Es sollte also nicht verwundern, dass 15 % der Befragten in Japan angeben, dass sie Warnmeldungen *oft* oder *immer* verpassen.

Neuseeland

Die Observability-Praktiken in Neuseeland zeichnen sich durch Business-Relevanz und durch klare, messbare Auswirkungen auf die Customer Experience aus. Beachtliche 82 % geben an, dass sich ihre Observability-Bemühungen positiv auf die Customer Experience auswirken, was deutlich über dem weltweiten Durchschnitt von 69 % liegt. Dieser Erfolg ist vermutlich auf die starke Fokussierung der Unternehmen auf die Customer Journey zurückzuführen. Denn in Neuseeland sagen deutlich mehr Befragte (48 %) als im Länderdurchschnitt (25 %), dass das Verständnis der kritischen User Journeys für die Gesamtgeschäftsstrategie *sehr wichtig* ist.

Die Zusammenarbeit zwischen den Sicherheits- und den Observability-Teams ist eine weitere Stärke Neuseelands. 90 % können bei Problemen mit der Performance von Anwendungen und Infrastruktur die Security-Ursachen genau bestimmen – eine ganze Menge mehr als im weltweiten Durchschnitt, der bei 65 % liegt. Und diese Zusammenarbeit scheint sich auszuzahlen: 74 % sagen, dass die funktionsübergreifende Teamarbeit zu weniger kundenrelevanten Incidents führt. Der Vergleichswert liegt bei 64 %.

Neuseeland hat außerdem eine deutliche Neigung zu KI. 44 % sind begeistert von den Vorteilen, die KI ihren Teams bieten kann, und 38 % nutzen bereits *oft* oder *immer* neue KI-Technologien wie autonom agierende KI – das sind mehr als doppelt so viele wie im weltweiten Durchschnitt. Das größte KI-Hindernis ist in Neuseeland nicht die Datenqualität, sondern der Mangel an Know-how und Fachkenntnissen: 50 % nennen mangelndes Fachwissen oder mangelndes Verständnis in den übrigen Teams als größtes Hindernis – der weltweite Vergleichswert liegt bei 40 %.

Trotz dieser Stärken bleibt Alarmmüdigkeit eine Herausforderung. 52 % sagen, dass sie mehr Zeit als nötig mit der Bearbeitung von Warnmeldungen verbringen, was darauf hindeutet, dass selbst fortgeschrittene Teams in diesem Bereich immer noch Reibungsflächen haben.

Singapur

In Singapur entwickeln sich die Observability-Praktiken rasant, der Schwerpunkt liegt eindeutig auf Geschwindigkeit und Effizienz. 64 % der Befragten geben hier an, dass der Observability-ROI in erster Linie davon abhängt, wie schnell das Troubleshooting bei Incidents ist – deutlich mehr als im internationalen Länderdurchschnitt (49 %). Darin zeigt sich eine schnell drehende IT-Kultur, für die schnelle Reaktionen unerlässlich sind.

Die Befragten des Inselstaats investieren kräftig in KI-gestützte Lösungen, vielleicht weil diese dem Bedarf an Tempo entgegenkommen. Überdurchschnittlich viele (61 %) sagen, dass sie AIOps *oft* oder *immer* in ihren Observability-Workflows einsetzen, und beachtliche 85 % geben an, dass sie KI regelmäßig im Rahmen ihrer täglichen Arbeit nutzen – fast 10 % mehr als im weltweiten Durchschnitt. Diese Zahlen deuten darauf hin, dass Singapur nicht nur mit KI experimentiert, sondern KI-Lösungen aktiv in die operativen Prozesse integriert.

Der Weg zu betrieblicher Effizienz ist jedoch nicht frei von Hindernissen. Namentlich der Tool-Wildwuchs stellt auch in Singapur eine große Herausforderung dar: 65 % der Befragten müssen feststellen, dass die Moral der Teams unter der Vielzahl unverbundener Tools leidet. Der größte Dämpfer ist aber nicht der Tool-Wildwuchs, sondern die Menge der Fehlalarme. Ganze 50 % der Befragten müssen eingestehen, dass sie mehr Zeit als nötig für die Bearbeitung von Warnmeldungen aufbringen. Das ist ein deutliches Zeichen dafür, dass die Teams trotz der Einführung hoch entwickelter Technologien Schwierigkeiten haben, Signale vom Rauschen zu trennen.

USA

Die Observability-Praxis in den Vereinigten Staaten bildet sich weitgehend in den Schlüsselmetriken des weltweiten Durchschnitts ab. Es gibt jedoch einige Bereiche, die abweichende Muster zeigen, insbesondere wenn es darum geht, ob und wie die Sicherheitsteams mit Observability-Daten arbeiten und wie die Unternehmen die Incident Response handhaben.

Die Security-Teams in den USA profitieren offenbar stark von Observability-Daten: 54 % der Befragten – also spürbar mehr als im weltweiten Durchschnitt von 47 % – geben an, dass Warnmeldungen einen *deutlichen* Einfluss auf Sicherheitsentscheidungen haben. Darüber hinaus zeigen sich die US-Befragten optimistisch, was die Möglichkeiten von KI betrifft, diesen Bereich weiter zu optimieren: 65 % sind der Überzeugung, dass sich KI positiv auf die Erkennung von Schwachstellen und Bedrohungen bei Anwendungen auswirken wird – der Vergleichswert des weltweiten Durchschnitts liegt bei 58 %. Diese Zahlen deuten darauf hin, dass sich die Funktionsbereiche Observability, KI und Cybersicherheit immer stärker aneinander ausrichten.

Allerdings sagen die befragten US-Amerikaner etwas häufiger (15 %) als der weltweite Durchschnitt (13 %), dass sie *oft* oder *immer* Warnmeldungen verpassen, und sie haben auch häufiger (16 %) als der Rest (11 %) Ausfälle aufgrund von verpassten Warnmeldungen zu verzeichnen. Mit dieser Warnmeldesituation dürfte auch zu tun haben, dass bei der Incident Response in den USA öfter Panikreaktionen vorherrschen. 12 % der Befragten müssen zugeben, dass sie *oft* oder *immer* in Panik geraten, wenn der Incident die Kundschaft betrifft. Der weltweite Durchschnitt liegt bei nur 9 %.

Vereinigtes Königreich

In Großbritannien und Nordirland ist Observability ein starker Produktivitätsfaktor. 75 % sagen, dass ihre Observability-Praktiken sich positiv auf die Effizienz der Beschäftigten auswirken. Dies deutet darauf hin, dass die britischen Teams ihre Observability-Daten offenbar erfolgreich einsetzen und damit Reibungsverluste reduzieren, Workflows optimieren und den Teams die Möglichkeit geben, sich auf wertschöpfende Aufgaben zu konzentrieren.

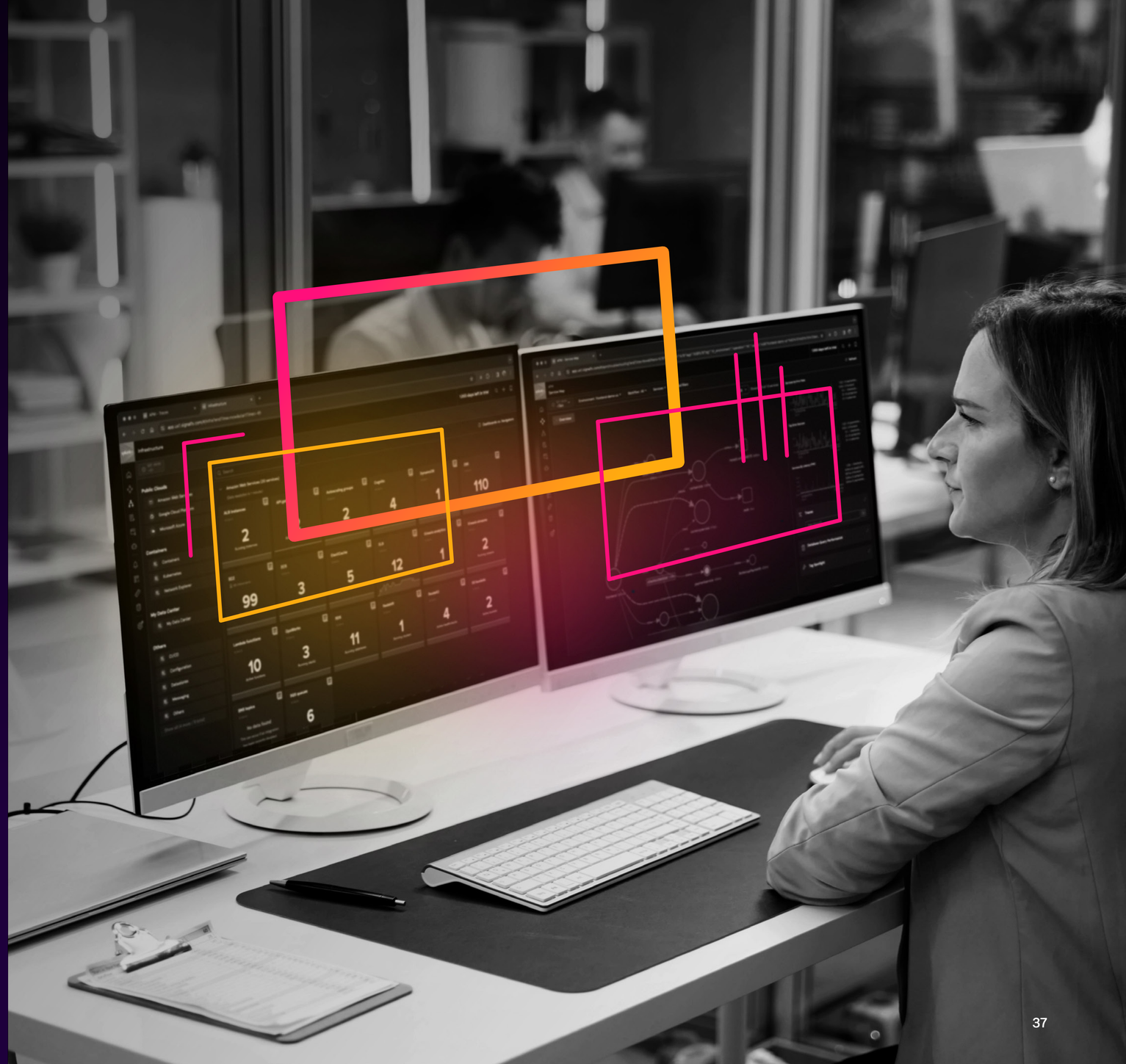
Zu KI nehmen die Befragten eine vorsichtig optimistische Haltung ein. 39 % sagen, dass sie von den KI-Vorteilen begeistert sind – also etwas mehr als der weltweite Durchschnitt von 36 % –, und fast die Hälfte (48 %) beschreibt sich selbst als optimistisch, möchte aber noch mehr Informationen einholen, bevor KI in vollem Umfang in den Teams etabliert wird. Troubleshooting und Fehler-Ursachen-Analyse werden als die Schlüsselbereiche angesehen, in denen KI-Funktionen den Unterschied machen könnten; 60 % erwarten von KI eine positive Wirkung auf diese Prozesse.

Dennoch bleiben Herausforderungen bestehen, insbesondere bei den Warnmeldungen. Mehr als die Hälfte (54 %) gibt an, dass die Menge der Fehlalarme in den Teams für Stress sorgt, und auch bei der Frage, was am meisten auf die Arbeitsmoral schlägt, stehen Fehlalarme ganz oben auf der Liste. Mit diesem Rauschen korrespondiert logischerweise eine Alarmhygiene, die eher suboptimal ist: 15 % – also etwas mehr als im weltweiten Durchschnitt – bekennen, dass sie Warnmeldungen *oft* oder *immer* ignorieren bzw. unterdrücken.

Während der Einsatz von OpenTelemetry dem weltweiten Durchschnitt entspricht (derzeit setzen 26 % OTel oft oder immer ein), sind in Großbritannien die Auswirkungen bei der Markenwahrnehmung besonders ausgeprägt: Mehr als drei Viertel (76 %) der Befragten, die OpenTelemetry zumindest manchmal nutzen, sagen, dass OpenTelemetry die Wahrnehmung ihrer Marke verbessert hat. Darin zeigt sich sehr deutlich, dass der strategische Nutzen moderner Observability-Tools weit über die rein technischen Ergebnisse hinausreicht.

Methodik

Oxford Economics befragte von Februar bis März 2025 insgesamt 1855 Fachleute aus ITOps und Engineering, von den Teams bis hinauf in die Führungsspitze: Entwickler, SREs, System Engineers und Infrastructure-Operations-Fachleute ebenso wie CTOs und CIOs. Die Befragten kommen aus Australien, Deutschland, Frankreich, Indien, Japan, Neuseeland, Singapur, dem Vereinigten Königreich und den USA. Vertreten sind damit 16 Branchen: Unternehmensdienstleistungen, Bau und Konstruktion, Konsumgüter, Bildungswesen, Finanzdienstleister, öffentliche Hand (Bund, Länder und Kommunen), Gesundheitswesen, Biowissenschaften, Fertigung, Technologie, Medien, Öl/Gas, Einzelhandel/Großhandel, Telekommunikation, Transport und Logistik sowie Versorgungsunternehmen.



Über Splunk

Splunk, ein Unternehmen von Cisco, macht die digitale Welt sicherer und resilienter. Führende Unternehmen nutzen unsere Plattform für einheitliche Security und Observability, um die Sicherheit und Zuverlässigkeit ihrer digitalen Systeme aufrechtzuerhalten. Unternehmen vertrauen auf Splunk, um zu verhindern, dass sich Sicherheits-, Infrastruktur- und Anwendungsprobleme zu größeren Vorfällen entwickeln, um Beeinträchtigungen durch digitale Störungen zu reduzieren und um die Transformation zu beschleunigen.

Bleiben Sie dran und reden Sie mit:

splunk>
a cisco company

25_CMP_report_state-of-observability-2025_v16_DE