orca security

Bericht zur Alarmmüdigkeit im Bereich Cloud-Sicherheit 2022

Das Ausmaß der öffentlichen Cloud-Alarmmüdigkeit, ihre Ursachen, Auswirkungen und mögliche Lösungen

In diesem Bericht

Zusammenfassung

Sicherheitsexperten sind alle mit der Alarmmüdigkeit nur allzu vertraut. Sie waren in der On-Premise-Welt damit konfrontiert, und jetzt müssen sie es in der Cloud bewältigen. Unternehmen setzen viele verschiedene Sicherheitstools ein, die Alarmmeldungen generieren. Dies überfordert die Sicherheitsteams, die jeden Tag Stunden damit verbringen müssen, die Alarmmeldungen zu prüfen, um festzustellen, welche Probleme zuerst behoben werden müssen.

Wie in der Fabel „Der Hirtenjunge und der Wolf“ findet eine Desensibilisierung statt, wenn die Zahl der bedeutungslosen und falsch-positiven Alarmmeldungen (Fehlmeldungen) zu groß wird, was dazu führt, dass Alarmmeldungen, die eigentlich Aufmerksamkeit verdienen, übersehen werden.

Zusammenfassung

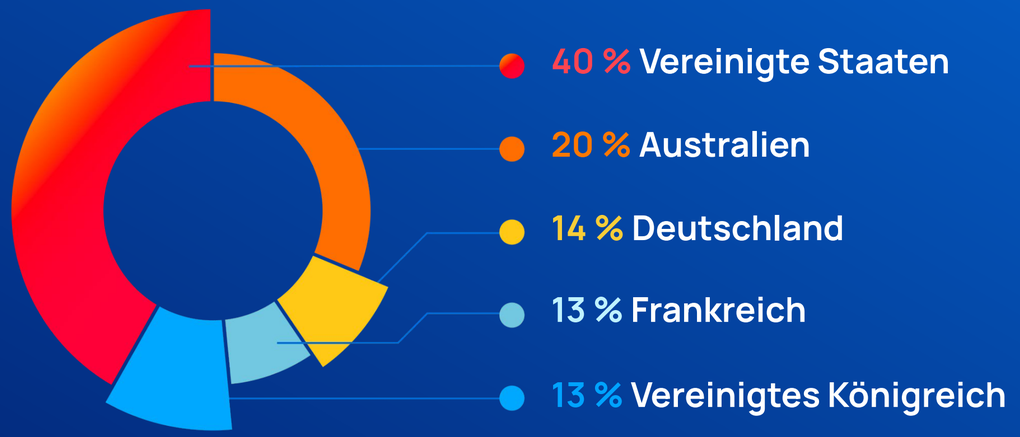
Die Umfrage

Um mehr über den aktuellen Stand der Alarmmüdigkeit, ihre Ursachen, Auswirkungen und die möglichen Lösungen herauszufinden, gab Orca Security eine weltweite Umfrage unter 813 IT-Entscheidungsträgern in fünf Ländern und zehn Branchen in Auftrag.

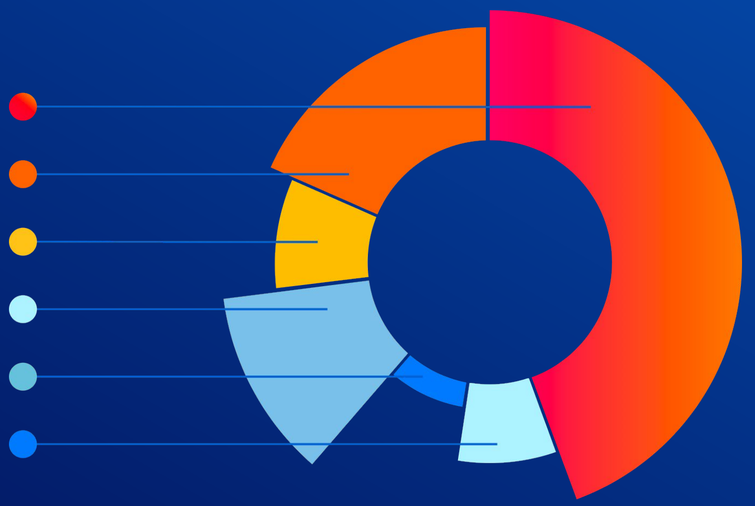
In diesem Bericht werden die globalen Ergebnisse erörtert.
Die wichtigsten Ergebnisse nach Ländern und Branchen sind im Anhang aufgeführt.

> Die Mehrheit der Befragten stammte aus Unternehmen mit **200–1.000 Beschäftigten** (79 %).
>
> Die meisten befragten Cloud-Sicherheitsteams bestanden aus **1 bis 50 Mitgliedern**.

Länder



Branche



Zusammenfassung

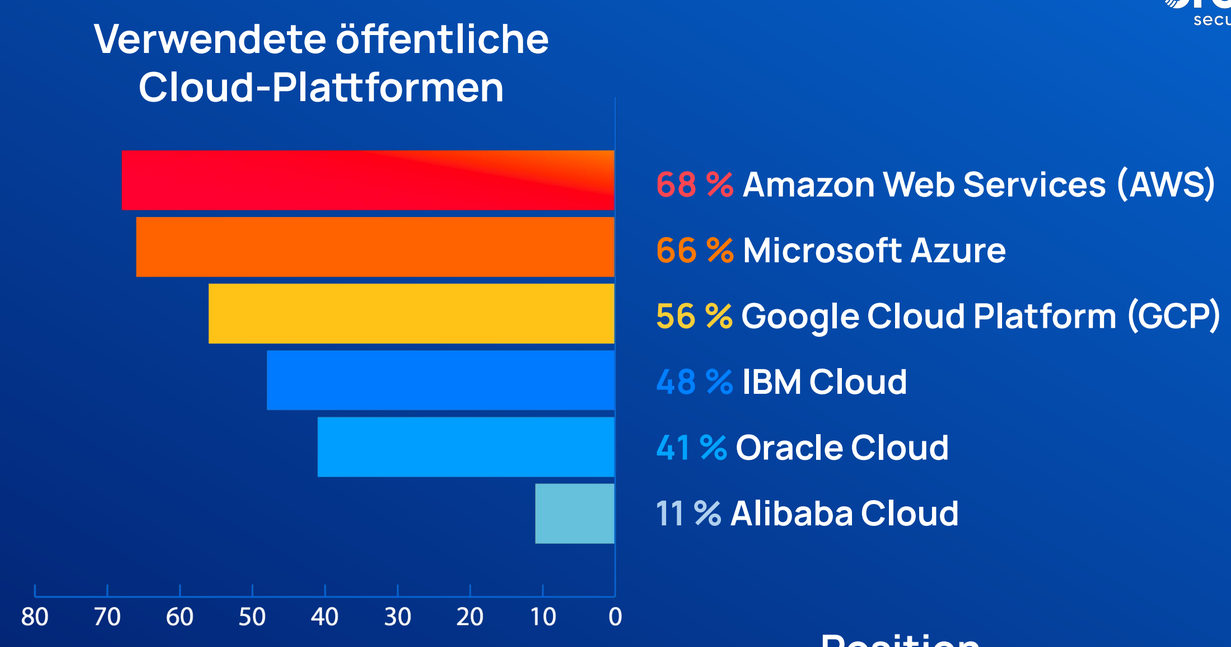
Die Befragten

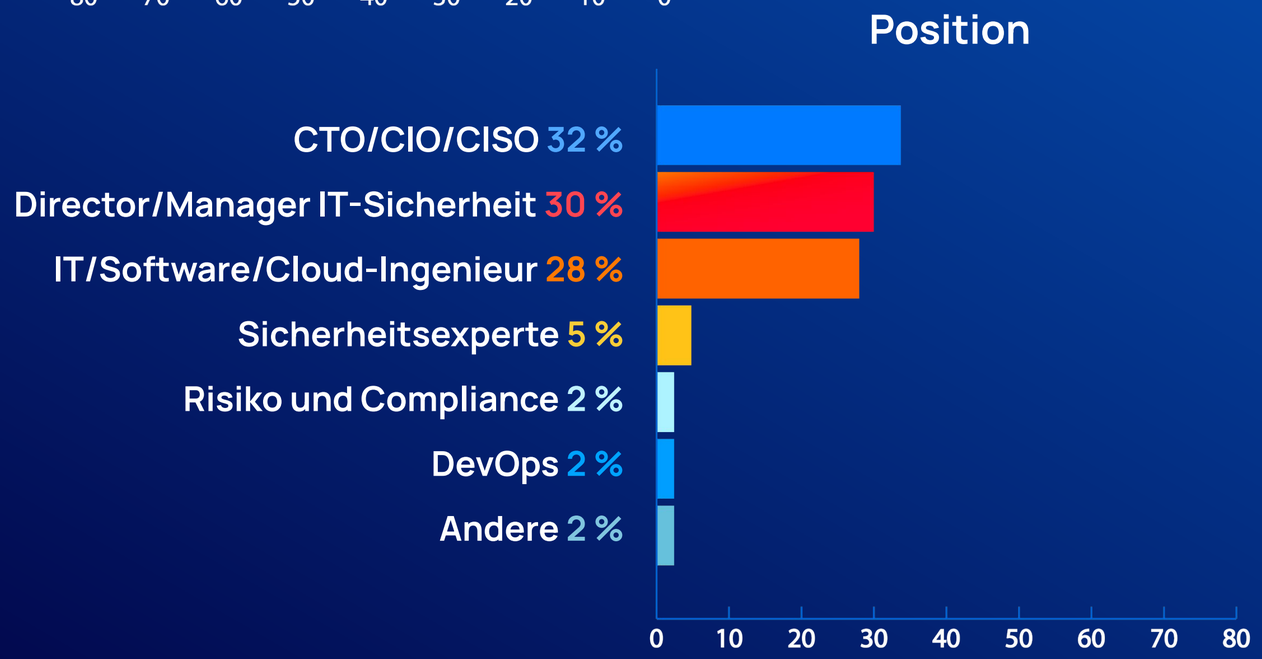
Um an der Umfrage teilzunehmen, mussten die Befragten mindestens 25 Cloud-Assets auf einer der großen öffentlichen Cloud-Plattformen haben. Die Mehrheit der Befragten (84 %) hatte mehr als 100 Cloud-Assets. Die meisten Befragten nutzen AWS, Azure und Google Cloud, dicht gefolgt von IBM Cloud und Oracle Cloud.

Die berufliche Position der Befragten reichte von Mitarbeitern (10 %) über Manager (61 %) bis hin zu Führungskräften (29 %).

> Die große Mehrheit (81 %) nutzt eine **Multi-Cloud-Strategie** mit mehr als einer Cloud-Plattform.

> 55 % der Befragten verwenden **3 oder mehr** öffentliche Cloud-Plattformen.





Zusammenfassung

Wichtigste Erkenntnisse

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 59 % de. Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 43 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind, und 49 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 56 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 62 % der Befragten gaben an, dass die Alarmmüdigkeit zur Personalwechsel beigetragen hat, und 60 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 55 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 41 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und 22 % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 57 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 95 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools **zuversichtlich oder sehr zuversichtlich** sind, auch wenn 43 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 97 % der Befragten geben an, dass sie **mit der Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 49 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

59 %

erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag

62 %

sagen, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat

95 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

1

Sicherheitsteams werden mit Alarmmeldungen überflutet

Sicherheitsteams werden täglich mit Alarmmeldungen überflutet. 59 % der Befragten erhalten mehr als 500 und 38 % mehr als 1.000 Sicherheitswarnungen für öffentliche Clouds pro Tag. Neben dem Erhalt neuer Alarmmeldungen müssen die Teams auch Alarmmeldungen verwalten, die noch behoben werden und noch nicht geschlossen wurden. 79 % der Befragten gaben an, dass sie zu einem bestimmten Zeitpunkt mehr als 500 Cloud-Sicherheitswarnungen offen haben, und 55 % gaben an, dass sie mehr als 1.000 offen haben.

Ein großer Teil des Arbeitstages eines Sicherheitsexperten besteht aus der Überprüfung und Priorisierung von Alarmmeldungen. Mehr als die Hälfte der Sicherheitsteams gab an, dass sie mehr als 20 % ihrer Zeit dafür aufwenden, und ein Viertel der Teams verbringt mehr als 40 % der Zeit mit der Entscheidung, welche Alarmmeldungen zuerst behandelt werden sollten.

Ein Tag im Leben eines Sicherheitsexperten:

- **59 %** erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag
- **56 %** verbringen mehr als 20 % ihres Arbeitstages mit der Überprüfung und Priorisierung von Alarmmeldungen
- **79 %** haben täglich mehr als 500 offene Cloud-Sicherheitswarnungen

Die Finanzbranche leidet am meisten

71 % der befragten Finanzdienstleister erhalten täglich mehr als 500 Sicherheitswarnungen für öffentliche Clouds, **85 %** haben mehr als 500 Sicherheitswarnungen für öffentliche Clouds offen, und **63 %** der Sicherheitsteams verbringen täglich mehr als 20 % der Zeit mit der Überprüfung und Priorisierung von Alarmmeldungen.
Dies deutet darauf hin, dass die Sicherheits- und Compliance-Kontrollen in der Finanzdienstleistungsbranche höher angesetzt sind.

2

Alarmmeldungen sind zu ungenau

Sicherheitsteams erhalten viele falsch markierte Probleme. Nicht weniger als 81 % der Befragten geben an, dass mehr als 20 % der Alarmmeldungen Fehlmeldungen sind.
Etwas weniger als die Hälfte (43 %) gab an, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind. Unabhängig davon müssen die Teams jede Alarmmeldung so behandeln, als sei sie eine echte Alarmmeldung, bis sie das Gegenteil beweisen können. Dies führt zu Zeitverschwendung und trägt zur Desensibilisierung bei.

Selbst wenn es sich nicht um Fehlmeldungen handelt, sondern um Alarmmeldungen mit geringer Priorität, die nicht sofort bearbeitet werden müssen, vergeuden sie Zeit, wenn die Teams sie von den wichtigen Alarmmeldungen trennen müssen. 49 % der Befragten geben an, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben, und sogar 83 % sagen, dass mehr als 20 % ihrer Alarmmeldungen eine niedrige Priorität haben.

Nur ein kleiner Teil der Alarmmeldungen ist tatsächlich kritisch und muss sofort beachtet werden – bei der Mehrheit der Befragten sind es sogar weniger als 10 %. Um jedoch diese 10 % der Alarmmeldungen unter den Hunderten von Alarmmeldungen mit niedriger Priorität und falsch-positiven Alarmmeldungen zu finden, müssen die Teams viel Zeit mit der Analyse und Untersuchung der Alarmmeldungen verbringen.

Der Hirtenjunge und der Wolf?

43 %

sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind

49 %

sagen, dass mehr als 40 % Alarmmeldungen mit niedriger Priorität sind

64 %

sagen, dass weniger als 10 % der Alarmmeldungen tatsächlich kritisch sind

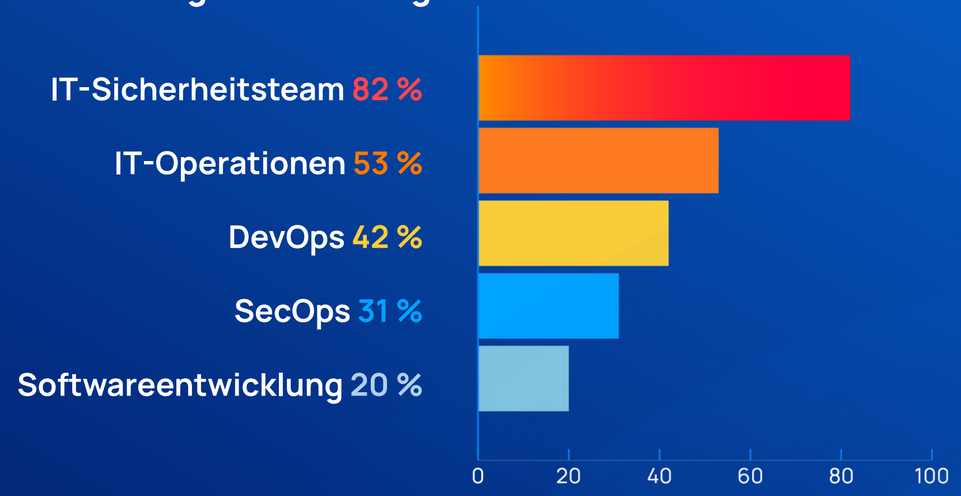
3

Abhilfemaßnahmen belasten die Sicherheitsteams

Neben der Entscheidung, welche Alarmmeldungen priorisiert werden müssen, tragen die Sicherheitsteams die größte Verantwortung für die Einstufung und Beseitigung von Alarmmeldungen. 82 % der Befragten gaben an, dass das IT-Sicherheitsteam und 31 %, dass SecOps für die Beseitigung von Alarmmeldungen verantwortlich sind. Die Software-Entwicklung scheint am seltensten in Anspruch genommen zu werden: Nur 20 % der Befragten gaben an, dass die Entwicklung für die Abhilfemaßnahmen verantwortlich ist.

Viele Sicherheitsprobleme in der Cloud sind nicht so einfach zu beheben. Nur 19 % der Befragten gaben an, dass die Behebung einer Alarmmeldung im Durchschnitt weniger als einen Tag dauert. 35 % gaben 1–2 Tage an, und fast die Hälfte aller Befragten gab an, dass die Behebung drei oder mehr Tage dauert.

Wer ist für die Prüfung und Behebung von Alarmmeldungen zuständig?



Sicherheitsteams tragen auch die größte Last bei der Behebung von Störungen

82 %

sagen, dass das IT-Sicherheitsteam für die Beseitigung von Alarmmeldungen zuständig ist

46 %

sagten, dass es 3 oder mehr Tage dauert, um eine Alarmmeldungen zu beheben

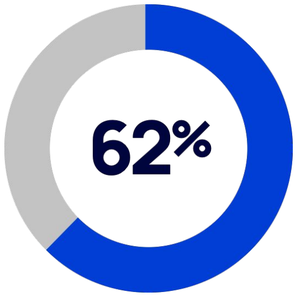
79 %

haben täglich mehr als 500 offene Cloud-Sicherheitswar nungen

4

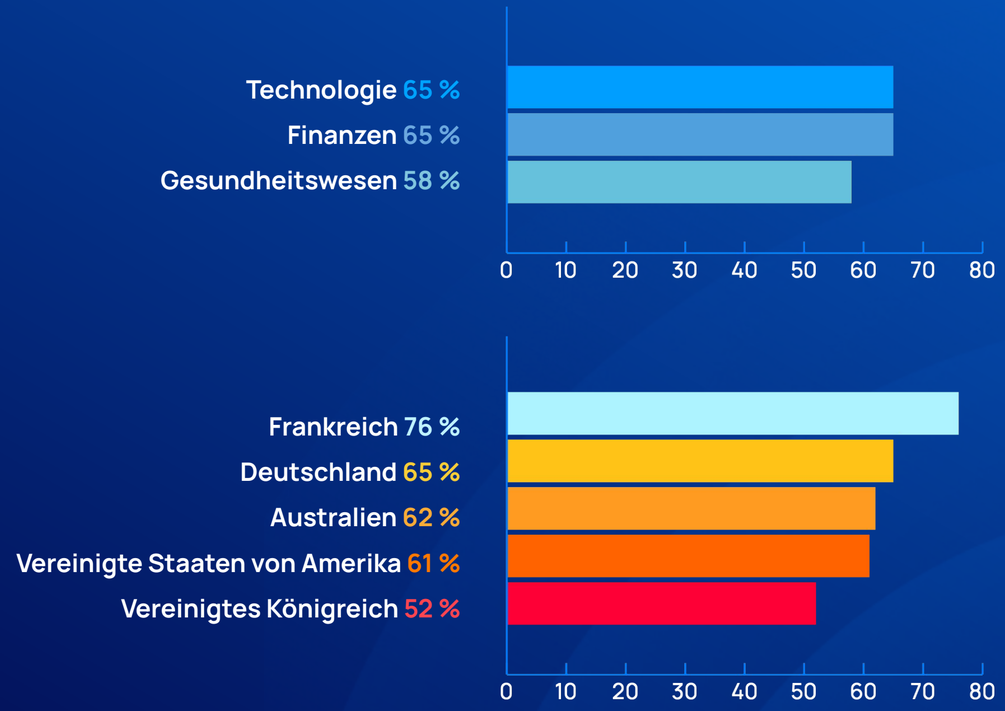
Sicherheitsteams sind zunehmend überlastet

Die schiere Anzahl von Alarmmeldungen mit vielen Fehlalarmen und Alarmmeldungen mit niedriger Priorität und nur einer kleinen Anzahl von Alarmmeldungen, die tatsächlich beachtet werden müssen, demoralisiert die Teams, überlastet sie und lässt sie ausbrennen. **62 % der Befragten gaben an, dass die Ermüdung durch Alarmmeldungen zu Personalwechsel in ihrem Unternehmen beigetragen hat**. Unabhängig von Land und Branche gibt die Mehrheit der Befragten an, dass die Alarmmüdigkeit dazu geführt hat, dass Mitarbeiter ihre Stelle verlassen haben. Das Vereinigte Königreich scheint jedoch am unteren Ende der Skala zu liegen, und Frankreich scheint das Problem am stärksten zu spüren.



von Befragten geben an, dass die Alarmmeldungen zu Personalwechsel in ihrer Organisation beigetragen haben.

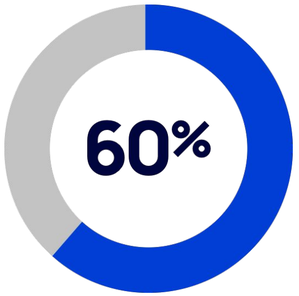
Die Mehrheit sagt, dass die Alarmmeldungen zu Personalwechsel beigetragen haben:



5

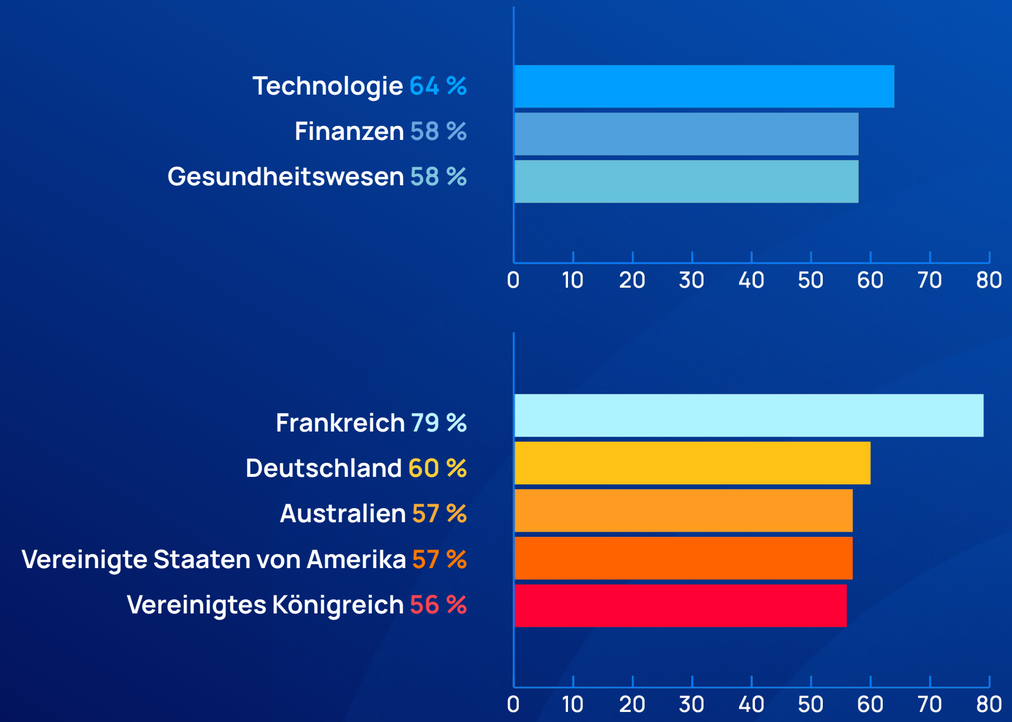
Alarmmüdigkeit führt zu internen Konflikten

Da die Beseitigung von Alarmmeldungen häufig in die gemeinsame Verantwortung von Sicherheit, IT und DevOps fällt, beeinträchtigt die Alarmmüdigkeit auch die interne Zusammenarbeit im Unternehmen. **60 % der Befragten gaben an, dass die Alarmmüdigkeit zu Konflikten zwischen ihren DevOps- und Sicherheitsteams geführt hat**.



der Befragten gaben an, dass die Alarmmüdigkeit zu Konflikten zwischen ihren DevOps- und Sicherheitsteams geführt hat.

Die Mehrheit sagt, dass die Alarmmüdigkeit zu organisatorischen Konflikten geführt hat:



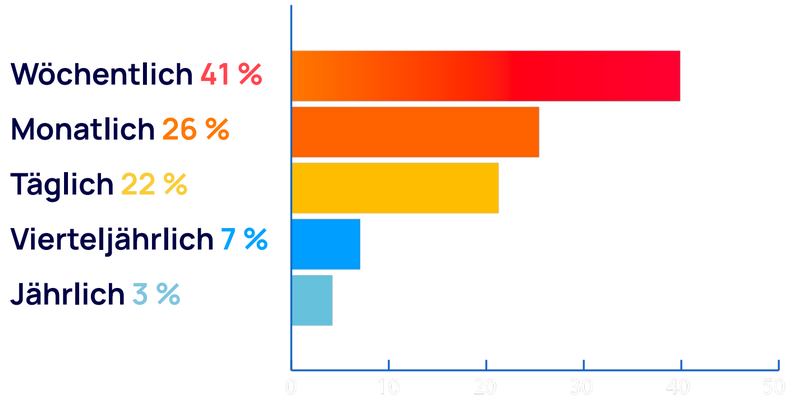
6

Kritische Alarmmeldungen werden übersehen

Aufgrund der schieren Anzahl nicht priorisierter Alarmmeldungen werden Sicherheitsexperten desensibilisiert, was dazu führt, dass Alarmmeldungen, die eigentlich sofortige Aufmerksamkeit erfordern, übersehen werden – mit möglicherweise katastrophalen Folgen.

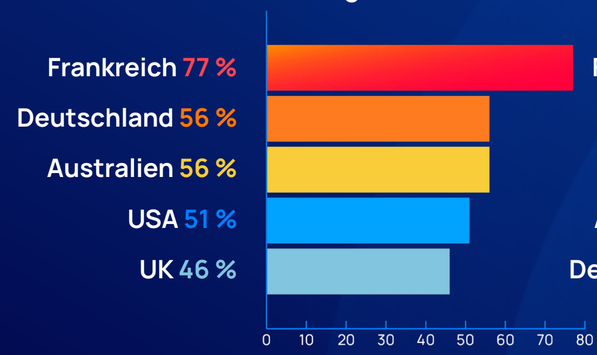
> Mehr als die Hälfte (55 %) der Befragten gab an, dass ihr Team in der Vergangenheit kritische Alarmmeldungen aufgrund einer ineffektiven Priorisierung der Alarmmeldungen übersehen hat. Von diesen Befragten gaben 22 % an, dass sie kritische Alarmmeldungen täglich verpassten, 41 % sagten wöchentlich und 26 % sagten monatlich.

Kritische Alarmmeldungen werden häufig übersehen

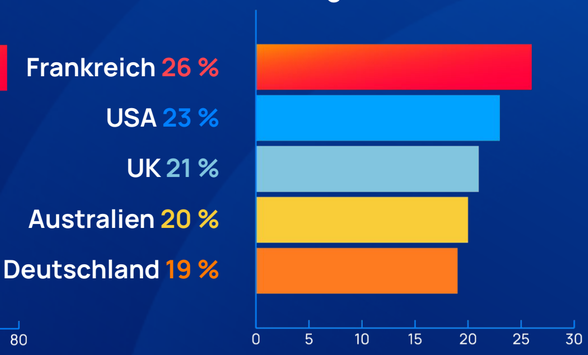


Nach Land

Verpasste kritische Alarmmeldungen:



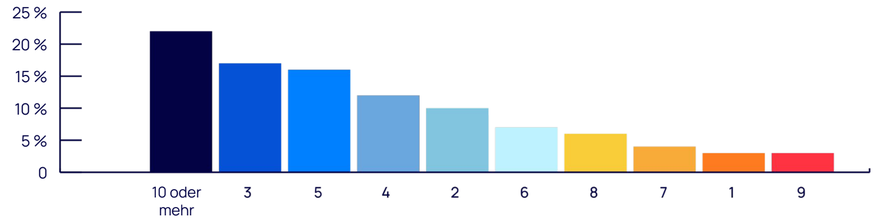
Täglich verpasste kritische Alarmmeldungen:



7

Isolierte Sicherheitstools verschärfen das Problem

Die überwiegende Mehrheit der Befragten nutzt drei oder mehr Sicherheitstools für öffentliche Clouds (87 %), 57 % sogar 5 oder mehr Tools. Die am häufigsten verwendeten Tools sind Netzwerkscanner (84 %), dicht gefolgt von nativen Sicherheitstools für Cloud-Plattformen (82 %).



Anzahl der öffentlichen Cloud-Sicherheitstools

Die Daten zeigen, dass die Sicherheitsteams mehr Alarmmeldungen erhalten, je mehr Tools sie einsetzen. Ein Teil dieser Korrelation lässt sich dadurch erklären, dass größere Unternehmen in der Regel über mehr Sicherheitstools und wahrscheinlich auch über mehr Cloud-Ressourcen verfügen, für die Alarmmeldungen generiert werden. Ein weiterer Faktor ist jedoch zweifellos, dass mehrere Tools die gleichen Probleme melden.

Interessanterweise scheint der Anteil der Fehlmeldungen ebenfalls zu steigen, je mehr Tools vorhanden sind, ebenso wie das Problem der Alarmmüdigkeit, was wiederum darauf hindeutet, dass mehrere Tools dieselben Probleme melden und damit Doppelarbeit für die Sicherheitsteams verursachen.

Mehr Tools = mehr Alarmmeldungen

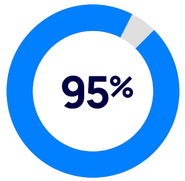
Mehr Tools = mehr Fehlmeldungen?

Mehr Tools = mehr Alarmmüdigkeit?

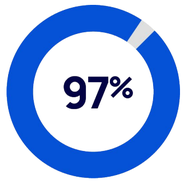
8

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

Die überwältigende Mehrheit der Befragten ist mit der Priorisierung der Alarmmeldungen und der Genauigkeit ihrer Sicherheitstools zufrieden und ist diesbezüglich zuversichtlich. Unsere Untersuchungen zeigen jedoch, dass dieses Vertrauen möglicherweise nicht unbedingt verdient ist. Setzen unsere Befragten die Messlatte zu niedrig an?

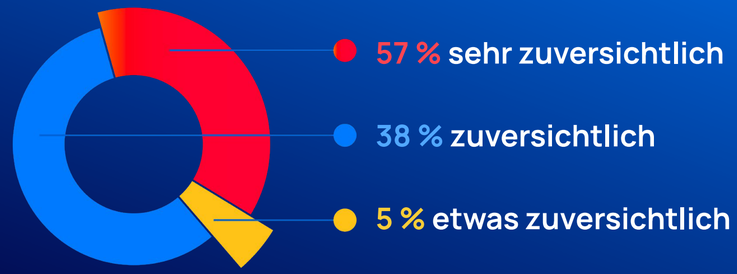


95 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich oder sehr zuversichtlich sind, auch wenn 43 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.

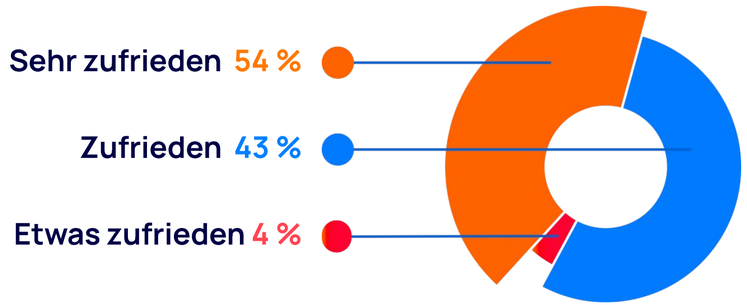


97 % der Befragten geben an, dass sie mit der Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden sind, auch wenn 49 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

Wie zuversichtlich sind Sie hinsichtlich der Genauigkeit Ihrer Cloud-Sicherheitswarnungen?



Wie zufrieden sind Sie mit der Fähigkeit Ihrer Cloud-Sicherheitslösungen, Alarmmeldungen zu priorisieren?



9

Wichtigste Empfehlungen

Die Umfrage zeigt, dass Alarmmüdigkeit ein großes Problem für die meisten Cloud-Sicherheitsteams darstellt. Dies führt nicht nur zu einer Personalwechsel, sondern auch dazu, dass kritische Alarmmeldungen – oft wöchentlich oder sogar täglich – übersehen werden. Die Verwendung mehrerer isolierter Tools zur Meldung von Cloud-Sicherheitswarnungen führt zu doppelten Alarmmeldungen und erhöht unnötig die Belastung der bereits überlasteten Sicherheitsteams.

Was können Unternehmen also tun, um das Problem der Alarmmüdigkeit zu lösen? Unternehmen müssen ihre Sicherheitsteams befähigen, intelligenter und nicht härter zu arbeiten.

Tool-Konsolidierung: Anstatt weitere isolierte Tools hinzuzufügen, sollten Sie die Tools auf weniger Plattformen konsolidieren, um doppelte Alarmmeldungen zu vermeiden und die Risikopriorisierung zu verbessern, indem Sie zentralisierte kontextbezogene Informationen nutzen, um gefährliche Risikokombinationen zu erkennen.

Verlangen Sie mehr von Ihren Sicherheitstools: Fragen Sie die Anbieter von Sicherheitslösungen, wie sie die Risiken priorisieren. Achten Sie darauf, dass sie zahlreiche Faktoren wie Schweregrad, Leichtigkeit der Ausnutzung, Zugänglichkeit und potenzielle Auswirkungen auf das Geschäft kombinieren.

Schützen Sie das Ziel und nicht den Eintrittspunkt: Vergewissern Sie sich, dass Sie wissen, wo sich Ihre wichtigsten Assets befinden, und finden Sie heraus, ob Ihr Sicherheitsanbieter die Risiken automatisch nach der potenziellen Gefährdung dieser Assets priorisiert.

Konzentration auf Angriffspfade: Sicherheitsteams müssen von der Untersuchung isolierter Alarmmeldungen zur Untersuchung und Priorisierung von Angriffsketten übergehen, um einen schnelleren Einblick in die Probleme zu erhalten, die zuerst behoben werden müssen.

Strategische Abhilfemaßnahmen: Anstatt zu versuchen, alle Alarmmeldungen in der Angriffskette zu beheben, sollten Sie zunächst die beheben, die die Kette unterbricht, um die unmittelbarste Gefahr einzudämmen.

Anhang

Wichtigste Erkenntnisse

Vereinigte Staaten

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 61 % der Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 48 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlalarme sind, und 54 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 63 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 61 % der Befragten geben an, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat, und 57 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 51 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 37 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und 23 % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 58 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 95 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools **zuversichtlich oder sehr zuversichtlich** sind, auch wenn 48 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 96 % der Befragten geben an, dass sie **mit der Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 54 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

61 %

erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag

61 %

geben an, dass die Alarmmüdigkeit zu Perosnalwechsel beigetragen hat

95 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

Wichtigste Erkenntnisse
UK

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 53 % der Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 45 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlalarme sind, und 54 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 52 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 52 % der Befragten geben an, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat, und 56 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 46 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 46 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und 21 % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 60 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 91 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools **zuversichtlich oder sehr zuversichtlich** sind, auch wenn 43 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 96 % der Befragten geben an, dass sie **mit der Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 54 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

53 %

erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag

52 %

geben an, dass die Alarmmüdigkeit zu Perosnalwechsel beigetragen hat

91 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

Wichtigste Erkenntnisse
Frankreich

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 61 % der Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 40 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind, und 43 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 45 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 76 % der Befragten geben an, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat, und 79 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 77 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 40 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und 26 % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 60 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 99 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools **zuversichtlich oder sehr zuversichtlich** sind, auch wenn 40 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 97 % der Befragten geben an, dass sie **mit der Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 43 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

61 %

erhaltean mehr als 500 Cloud-Sicherheitswarnungen pro Tag

76 %

geben an, dass die Alarmmüdigkeit zu Perosnalwechsel beigetragen hat

99 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

Wichtigste Erkenntnisse

Deutschland

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 54 % der Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 41 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind, und 48 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 50 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 65 % der Befragten gaben an, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat, und 60 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 56 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 54 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und 19 % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 43 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 95 % der Befragten geben an, dass sie hinsichtlich der **Genauigkeit ihrer Sicherheitstools zuversichtlich oder sehr zuversichtlich** sind, auch wenn 41 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 96 % der Befragten geben an, dass sie mit der **Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 48 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

54 %

erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag

65 %

geben an, dass die Alarmmüdigkeit zu Perosnalwechsel beigetragen hat

95 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

Wichtigste Erkenntnisse

Australien

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 61 % der Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 36 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind, und 42 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 56 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 62 % der Befragten gaben an, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat, und 57 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 56 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 39 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und 20 % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 61 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 94 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools **zuversichtlich oder sehr zuversichtlich** sind, auch wenn 36 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 97 % der Befragten geben an, dass sie **mit der Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 42 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

61 %

erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag

62 %

geben an, dass die Alarmmüdigkeit zu Perosnalwechsel beigetragen hat

94 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

Wichtigste Erkenntnisse

Finanzdienstleistungen global

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 71 % der Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 42 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind, und 51 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 63 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 65 % der Befragten gaben an, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat, und 58 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 61 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 35 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und [illegible] % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 58 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 91 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools **zuversichtlich oder sehr zuversichtlich** sind, auch wenn 42 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 94 % der Befragten geben an, dass sie mit der **Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 51 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

71 %

erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag

65 %

geben an, dass die Alarmmüdigkeit zu Perosnalwechsel beigetragen hat

91 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

Wichtigste Erkenntnisse

Gesundheitswesen global

Alarmmüdigkeit nach Zahlen:

- **Sicherheitsteams werden mit Cloud-Sicherheitswarnungen überschwemmt:** 53 % der Befragten erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag.
- **Eine große Anzahl von Alarmmeldungen ist ungenau oder unnötig:** 32 % geben an, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind, und 45 % sagen, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.
- **Die Überprüfung und Priorisierung von Alarmmeldungen ist eine wichtige Aufgabe:** 48 % verbringen mehr als 20 % ihres Arbeitstages damit, Alarmmeldungen zu überprüfen und zu entscheiden, welche zuerst bearbeitet werden sollen.

Alarmmüdigkeit führt zu Personalwechsel und verpassten kritischen Alarmen:

- **Alarmmüdigkeit führt zu Burnout, Personalwechsel und internen Konflikten:** 58 % der Befragten gaben an, dass die Alarmmüdigkeit zu Personalwechsel beigetragen hat, und 58 % sagten, dass die Alarmmüdigkeit zu internen Konflikten geführt hat.
- **Kritische Alarmmeldungen werden verpasst, oft auf täglicher und wöchentlicher Basis:** Von den 48 % der Befragten, die angaben, dass kritische Alarmmeldungen übersehen werden, gaben 41 % an, dass die Alarmmeldungen wöchentlich übersehen werden, und 34 % sagten, dass dies täglich geschieht.

Wird die Messlatte für Sicherheitstools zu niedrig angesetzt?

- 53 % haben **5 oder mehr öffentliche Cloud-Sicherheitstools**.
- 97 % der Befragten geben an, dass sie hinsichtlich der Genauigkeit ihrer Sicherheitstools **zuversichtlich oder sehr zuversichtlich** sind, auch wenn 32 % sagen, dass mehr als 40 % ihrer Alarmmeldungen Fehlmeldungen sind.
- 97 % der Befragten geben an, dass sie **mit der Priorisierung der Risiken durch ihre Sicherheitstools zufrieden oder sehr zufrieden** sind, auch wenn 45 % der Befragten angeben, dass mehr als 40 % der Alarmmeldungen eine niedrige Priorität haben.

53 %

erhalten mehr als 500 Cloud-Sicherheitswarnungen pro Tag

58 %

geben an, dass die Alarmmüdigkeit zu Perosnalwechsel beigetragen hat

97 %

sind hinsichtlich der Genauigkeit ihrer Sicherheitstools zuversichtlich?

Über Orca Security

Orca Security bietet sofortige Sicherheit und Compliance für AWS, Azure und GCP – ohne Abdeckungslücken, ohne Alarmmüdigkeit und ohne Betriebskosten für Agenten oder Sidecars. Vereinfachen Sie die Cloud-Sicherheitsoperationen mit einer einzigen CNAPP-Plattform für Workload- und Datenschutz, Cloud Security Posture Management (CSPM), Schwachstellenmanagement und Compliance.

Orca Security priorisiert Risiken nach dem Schweregrad des Sicherheitsproblems, der Zugänglichkeit und den Auswirkungen auf das Unternehmen. Dies hilft Ihnen, sich auf die kritischen Alarmmeldungen zu konzentrieren, die am wichtigsten sind. Orca Security genießt das Vertrauen globaler Innovatoren, darunter Databricks, Autodesk, NCR, Gannett und Robinhood.

Eröffnen Sie Ihr erstes Konto in wenigen Minuten:
https://orca.security oder führen Sie die kostenlose Cloud-Risikobewertung durch.