

Schließen von Security-Operations-Lücken mit MDR

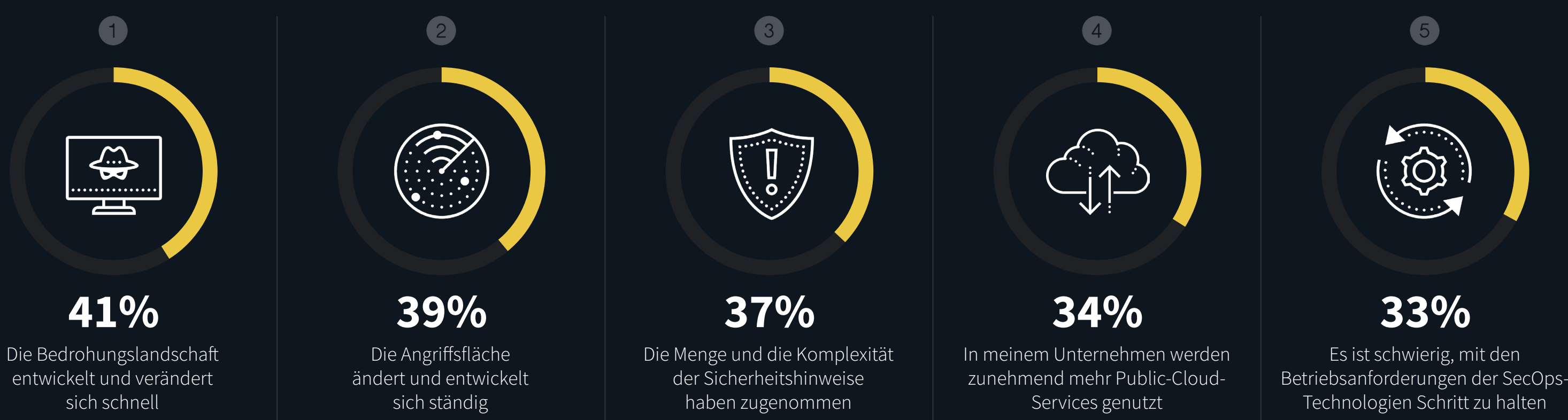
Da das eskalierende Risiko schwerwiegender Cyberangriffe sowohl Aufmerksamkeit als auch Budget von den Kerngeschäftsziele ablenkt, müssen Unternehmen ihre Cybersicherheitsprogramme verstärken. Ein zentraler Bestandteil aller Cybersicherheitsprogramme ist der Bereich Security Operations (SecOps), der für das Monitoring und den Schutz aller Facetten der digitalen Angriffsfläche verantwortlich ist.

Mehr Schwierigkeiten bei Security Operations trotz Investitionen



MEHR ALS DIE HÄLFTE der Befragten gibt an, dass SecOps heute schwieriger ist als vor zwei Jahren.

» Die fünf wichtigsten Gründe, warum SecOps schwieriger ist



Überdenken von Programmstrategien

Der Umfang und die Komplexität der Angriffsflächen und Bedrohungslandschaft haben genauso zugenommen wie die Nutzung von Sicherheitskontrollen, die Tausende von Warnmeldungen und enorme Mengen an Sicherheitsdaten erzeugen. Sicherheitsteams überdenken den allgemeinen Programmbetrieb, um Ressourcen- und Risikodaten von IT- und Geschäftsbereichsteams weiter zu integrieren, damit sie sich auf die Bedrohungen konzentrieren können, die das größte Risiko für die Unternehmensziele darstellen.

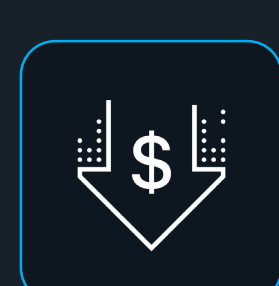


der Unternehmen arbeiten entweder bereits mit einem MDR-Anbieter zusammen oder planen eine solche Zusammenarbeit in den nächsten 12 Monaten.



dieser Unternehmen planen, die MDR-Nutzung in den kommenden 12 Monaten zu erweitern.

» Wichtige Werttreiber für MDR-Projekte



BETRIEBLICHE VERBESSERUNG UND EFFIZIENZ

MDR kann Unternehmen dabei helfen, die Gesamtkosten für Security Operations in verschiedenen Bereichen wie Infrastruktur, Personal und Management zu senken. Die Lösung kann zudem das Problem der „Alarmmüdigkeit“ beheben und die Wahrscheinlichkeit erhöhen, dass falsch positive Ergebnisse deutlich reduziert werden.



VERBESSERTE CYBERSICHERHEITSEFFIZIENZ UND GERINGERE RISIKEN

Mit MDR können Unternehmen bereits bestehende Bedrohungen stoppen, die Erkennung potenzieller Bedrohungen und erweiterter persistenter Angriffe verbessern, eine proaktive Bedrohungssuche aktivieren und stärkere Kontrollen zur Erkennung und Verhinderung zukünftiger Angriffe einsetzen.

» Was sind die Hauptgründe, aus denen Ihr Unternehmen Managed Services nutzt oder deren Nutzung plant?



55%

Fokus: Mein Unternehmen möchte, dass sich das Sicherheitspersonal auf strategischere Sicherheitsinitiativen konzentriert, anstatt Zeit mit Aufgaben für Security Operations zu verbringen.



52%

Services: Mein Unternehmen denkt, dass Serviceanbieter die Aufgaben im Bereich Security Operations besser erledigen können als wir.



49%

Erweiterung: Mein Unternehmen ist der Ansicht, dass ein Serviceanbieter unser SOC-Team in puncto Security Operations ergänzen kann.



42%

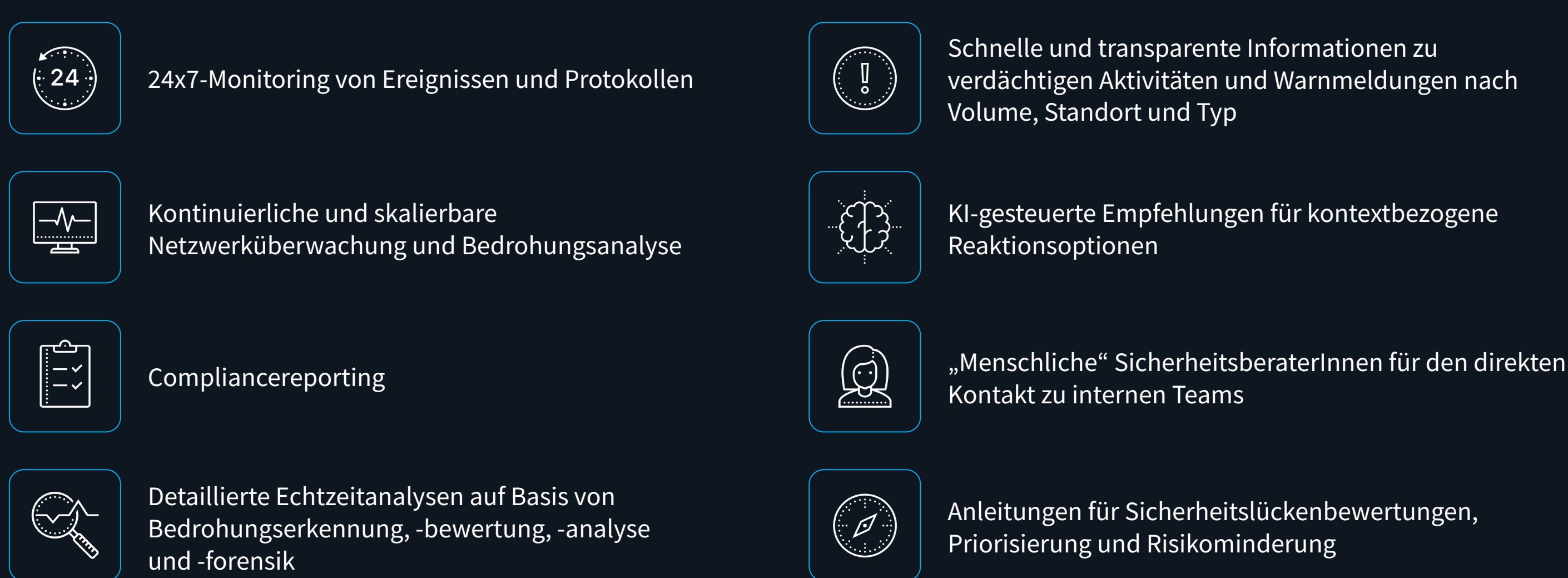
Kompetenzen: Mein Unternehmen verfügt im Bereich Security Operations nicht über die benötigten Fähigkeiten.

“Viele MDR-Lösungen der „Generation 1.0“ wurden für ein anderes Zeitalter entwickelt und implementiert, in dem es weniger Daten, weniger Bedrohungen und einfachere Erkennungsmaßnahmen gab.“

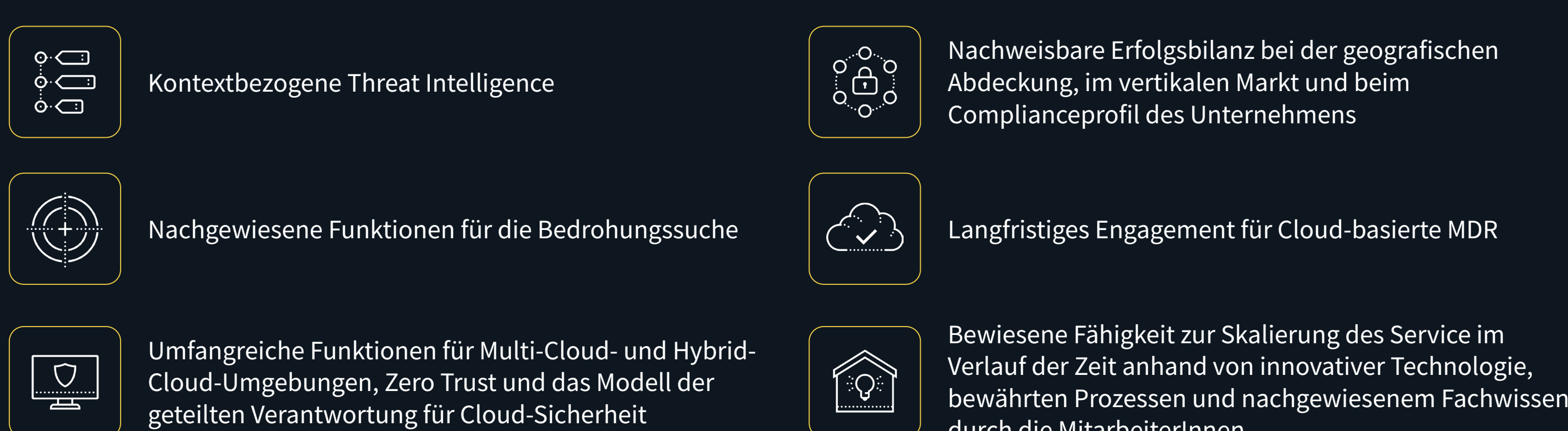
- Dave Gruber, ESG Principal Analyst

Neue Anforderungen für MDR

„Viele MDR-Lösungen der „Generation 1.0“ wurden für ein anderes Zeitalter entwickelt und implementiert, in dem es weniger Daten, weniger Bedrohungen und einfachere Erkennungsmaßnahmen gab. Die nächste Generation von MDR-Lösungen muss darauf ausgelegt sein, eine vielfältigere Angriffsfläche zu schützen, komplexere Bedrohungen zu erkennen und einen stärker risikozentrierten Ansatz zur Priorisierung und Risikominderung zu nutzen.“



Angesichts der großen Anzahl potenzieller Serviceanbieter, die einige, viele oder sogar alle outgesourceten MDR-Funktionen bereitstellen können, **sollten Unternehmen nach Partnern suchen, die Folgendes bieten:**



Die ganze Wahrheit

Da das eskalierende Risiko schwerwiegender Cyberangriffe sowohl Aufmerksamkeit als auch Budget von den Kerngeschäftsziele ablenkt, müssen Unternehmen ihre Cybersicherheitsprogramme verstärken. Auch wenn die Anwendungsbeispiele unterschiedlich sind, nutzen die meisten Unternehmen MDR-Serviceanbieter, um ihre Programme zu erweitern und zu skalieren.

Der Ansatz von Dell Technologies für Managed Detection and Response kombiniert flexible, intelligente und skalierbare Technologie mit erfahrenen CybersicherheitsexpertInnen und hilft Unternehmen jeder Größe und mit jedem Ressourcenprofil dabei, ihre Sicherheitsprogramme zu beschleunigen und zu verstärken.

[WEITERE INFORMATIONEN](#)

DELLTechnologies