Vodafone Business Managed Detection and Response

Schützen Sie Ihr Unternehmen mit professioneller Cybersicherheit.

Google Cloud

vodafone business

Die Bedrohungen verändern sich: Bereiten Sie sich vor.

Kleine und mittlere Unternehmen stehen im Zentrum von Cyberangriffen. Die Bedrohungen werden immer komplexer und hartnäckiger. Anders als größere Organisationen haben diese Unternehmen vielleicht Sicherheitslücken und begrenzte Ressourcen, um sich vor Anrgiffen zu schützen. Dafür brauchen Unternehmen die passenden Teams, das Fachwissen und Zeit. Nur so können sie sich gegen immer raffiniertere, häufigere und gezieltere Angriffe verteidigen.

Cyberkriminelle wissen genau, wo Schwachstellen sind. Schon ein einziger erfolgreicher Anrgiff kann ein Unternehmen viel Geld kosten. Dazu können rechtliche Konsequenzen Schäden für den Ruf des Unternehmens bedeuten. Allesamt große Herausforderungen für kleine und mittlere Unternehmen.

Genau hier hilft Ihnen Vodafone Business Managed Detection and Response. Es schützt Ihr Unternehmen proaktiv vor Cyberbedrohungen, erfüllt Compliance-Anforderungen und sorgt für einen stabilen Betrieb – ohne, dass Sie ein eigenes Security Operations Center (SOC) aufbauen müssen.

Was ist Managed Detection and Response (MDR)?

Unser MDR-Service ist eine umfassende, gemanagte Cybersicherheits-Lösung für mittelständische Unternehmen. Sie bekommen Sicherheitsfunktionen auf Enterprise-Niveau, die genau auf ihre kritischen Bedürfnisse zugeschnitten sind. Der Service umfasst: Überwachung rund um die Uhr, Bedrohungserkennung, umfassendes Incident-Management sowie Analysen und Reaktionen von Expert:innen.

Die Basis des Services sind unsere Sicherheitsexpert:innen und die Google SecOps-Plattform. Googles KI-Funktionen erkennen Bedrohungen, priorisieren und stoppen Bedrohungen schneller – durch intelligente Automatisierung und vorausschauende Analysen. Wir nutzen außerdem „User and Entity Behaviour Analytics“, UEBA. So können wir ungewöhnliches oder riskantes Verhalten schneller erkennen. Das sind z.B. Insider-Bedrohungen oder kompromittierte Konten. Unsere lokale SOC-Analyst:innen betreuen Sie dabei immer in Ihrer Landessprache. Die Kombination aus den globalen Threat-Intelligence-Kapazitäten von Vodafone und Mandiant bedeutet: MDR erkennt und reagiert effektiv auf bekannte und neue Bedrohungen.

Eine einfache, zugängliche und intelligente Lösung für Ihre Cyber-Herausforderungen

Umfassende Transparenz
Wir behalten die gesamte Angriffsfläche im Blick. Das heißt: wir erkennen und neutralisieren bekannte und unbekannte Bedrohungen.

Schnelle Identifizierung und Lösung
Überwacht Ihre IT-Umgebung kontinuierlich und erkennt verdächtige Aktivitäten frühzeitig. So reagieren wir schnell und gezielt auf Bedrohungen – unterstützt durch KI.

Kompetete Expert:innen
Wir haben über 30 Jahre Erfahrung im Bereich Cybersicherheit. Dazu nutzen wir Spitzentechnologie von Google SecOps und die marktführende Bedrohungsanalyse von Mandiant.

Erweiterung Ihres Teams
Ein gemeinsames Betriebsmodell und ein tiefgreifendes Verständnis Ihres Umfeldes und Ihrer kritischen Infrastruktur führen zu weniger Fehlalarmen, umsetzbaren Erkenntnissen und einer schnelleren Fehlerbehebung.

Globale Einblicke, lokale Expertise
Sie profitieren von unseren globalen Fähigkeiten zur Bedrohungsanalyse. Dazu bekommen Sie wichtige Erkenntnisse, die Unternehmen wie Ihres betreffen – von unserem zentralen SOC und lokalen Teams.

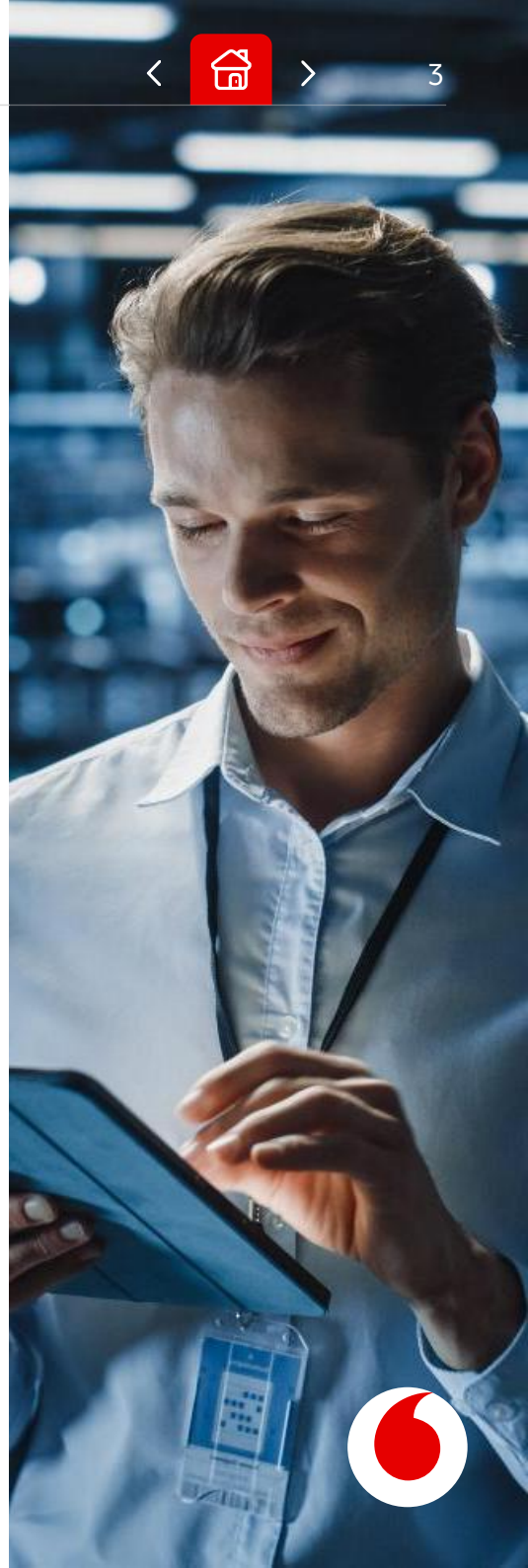
Alles wichtige immer im auf einen Blick
Sie bekommen alle wichtigen Infos über ein einziges Service-Dashboard. Dort können Sie auch direkt unsere SOC-Teams kontaktieren.

Einfache, skalierbare Preisgestaltung
Sie zahlen ganz einfach pro Nutzer:in. Das heißt: Sie bekommen planbare Kosten und haben keine unerwünschte Kostenexplosionen. Auch nicht, wenn Ihr Geschäft wächst.

Optimierte Investitionen
Sie können Ihre bisherigen Sicherheits-Tools und Technologien nutzen. So bekommen Sie mehr Nutzen und Einsichten aus Ihren Sicherheits-Investitionen.

Wichtige Sicherheitsereignisse auf einen Blick
Durch Google SecOps und Mandiant Intelligence bekommen Sie KI-gestützte Analysen. So haben Sie die wichtigsten Bedrohungen imme rim Blick.

Unterstützt mehrere Anbieter
Sie können MDR mit marktführenden Anbietern von Cybersicherheitslösungen integrieren. Dazu gehören , wichtige Endpoint Detection and Response-Tools: z. B. Microsoft Defender, CrowdStrike, Trend Micro oder SentinelOne. Aber auch Cloud-Anbieter, wie AWS, Azure, Google Cloud und Anbieter von Netzwerksicherheitslösungen, wie Zscaler.



Auf einer leistungsstarken Technologieplattform aufgebaut

MDR überwacht Ihre Umgebungen dauerhaft mit Technologie von Google SecOps, Googles SIEM- und SOAR. Das heißt: mit modernsten KI-Tools erfasst das System Daten aus Sicherheitstools und korreliert Bedrohungssignale. So können unsere erfahrenen Analyst:innen Vorfälle schnell untersuchen und darauf reagieren. Das Ganze wird vollständig von Vodafone verwaltet und bietet eine optimierte Erkennung und Reaktion auf Bedrohungen, ohne dass Sie ein eigenes SOC aufbauen müssen.

Transparenz und Kontrolle auf Knopfdruck

Vodafone Business CyberHub:

24/7 Sichtbarkeit

Sie können immer auf Vorfälle, Warnmeldungen, laufende Aktivitäten und wichtige Kennzahlen zugreifen.

Einfachheit und Kontrolle

Ein benutzer-freundliches Portal, auf dem Sie Supportanfragen stellen und direkt unser SOC-Team kontaktieren können.

Berichterstellung und Dashboards

Zugang zu fortschrittlichen Reporting-Tools, einschließlich monatlicher Standardberichte. Darin bekommen Sie detaillierte Einblicke in Ihre individuelle Umgebung.

Drei Schritte zu 360-Grad-Schutz mit Vodafone Business MDR

Zur Lösung gehören zentrale und lokale SOC-Teams, die Managed Security Services bereitstellen. Dabei kombinieren wir fortschrittliche Datenanalyse mit menschlicher Expertise. So bekommen Sie einen robusten Schutz rund um die Uhr:

1 Protokollerfassung und Ereigniskorrelation

- **Sichere Datenerfassung:** Vodafone Business MDR erfasst Sicherheitsprotokolle nahezu in Echtzeit aus vielen Quellen. Das sind z. B. Endpunkte, Mobilgeräte, Firewalls, Cloud-Anwendungen (z. B. AWS, Office 365), Netzwerke, Server, Betriebssysteme und Identitätsmanagement-Tools (z. B. Okta).
- **Datenverarbeitung:** Der Dienst nutzt Google SecOps SIEM, um große Mengen an Sicherheitsdaten auszuwerten. SecOps normalisiert, aggregiert und korreliert – und wandelt Rohdaten so in verwertbare Warnmeldungen um. Durch KI erkennt MDR ungewöhnliche Muster in verschiedenen Datenquellen besonders schnell.

2 Analyse und Überwachung

- **Sicherheitsvorfälle wurden erkannt:** Unsere Systeme und Expert:innen erkennen Sicherheitsvorfälle. KI und klare Regeln machen aus gesammelten Daten verständliche Sicherheitswarnungen.
- **SecOps:** Die SecOps-Erkennungs-Engine nutzt fortschrittliche Funktionen. Dazu gehören von Google kuratierte Erkennungen und auf der Primärforschung von Mandiant basierende Erkennungen. So identifizieren wir neue und aktive Bedrohungen schnell.
- **Verhaltensanalyse :** User and Entity Behaviour Analytics (UEBA) weiß durch maschinelles Lernen, wie sich Nutzer:innen normalerweise verhalten. Weicht dieses Verhalten ab, schlägt das System Alarm – zum Beispiel bei kompromittierten Konten oder internen Bedrohungen.
- **KI-gestützte Analyse:** Wir nutzen hochwertige Bedrohungsdaten aus Quellen wie Googles globaler Telemetrie, Mandiant Insights und VirusTotal. Diese Daten nutzen wir für Erkennung, Analyse und Reaktion. So bekommen wir wichtige Infos zu Angriffstaktiken. KI hilft uns dann dabei, diese Daten mit globalen Mustern abzugleichen – und Angriffe vorherzusagen, bevor sie stattfinden.

3 Bedrohungsanalyse und Reaktion

- **Professionelle Bedrohungsanalyse:** Unsere erfahrenen Analyst:innen prüfen, klassifizieren und priorisieren erkannte Sicherheitsvorfälle anhand ihrer Schwere des unmittelbaren Risikos und der potenziellen Auswirkungen auf die Organisation.
- **Intelligente Automatisierung:** Google SecOps Google SecOps SOAR automatisiert Workflows zur Vorfallreaktion mithilfe von Playbooks, die sich in Tools von Drittanbietern integrieren lassen, wodurch die Reaktionszeiten erheblich verkürzt werden. Analysten können automatisierte Maßnahmen direkt über die SOAR-Konsole auslösen.
- **Expert:innen-Wissen im Einsatz:** Die Automatisierung sorgt für mehr Tempo. Unsere SOC-Analyst:innen prüfen komplexe Bedrohungen, bestätigen Warnmeldungen und begleiten Sie bei den nächsten Schritten.
- **Behebung:** Unser SOC-Team kümmert sich bei Bedarf um konkrete Schutzmaßnahmen. Dazu gehören etwa das Isolieren von Endgeräten, das Sperren schädlicher IP-Adressen oder das Beenden von Nutzersitzungen.

Warum Vodafone Business MDR wählen?

Über unsere zentralen und lokalen SOC-Teams bekommen Sie Managed Security Services. Wir kombinieren fortschrittliche Datenanalyse mit menschlicher Expertise. So schützen wir Sie rund um die Uhr:

- Lückenlose Überwachung des Netzwerks
- Schnellere Reaktion und wirksame Behebung von Sicherheitsvorfällen
- Das MDR-Team steht Ihnen rund um die Uhr für Unterstützung und Beratung bei Vorfällen zur Verfügung
- Onboarding Unterstützung für den MDR-Service
- Sicherheitsprotokolle und Ereigniskorrelation in Echtzeit
- Überprüfung und Benachrichtigung bei Sicherheitsvorfällen in Echtzeit
- Geräteprotokoll-Überwachung und Benachrichtigung bei Protokollausfällen
- Sicherer Webportalzugriff mit Live-Service-Dashboard
- Standardmonatsberichte & Berichte nach Vorfällen

Außerdem helfen wir Ihnen, gesetzeskonform zu bleiben und jederzeit auditbereit zu sein. Wir unterstützen branchenspezifische Vorgaben wie DSGVO und NIS2, liefern automatische Berichte und behalten neue Anforderungen im Blick.

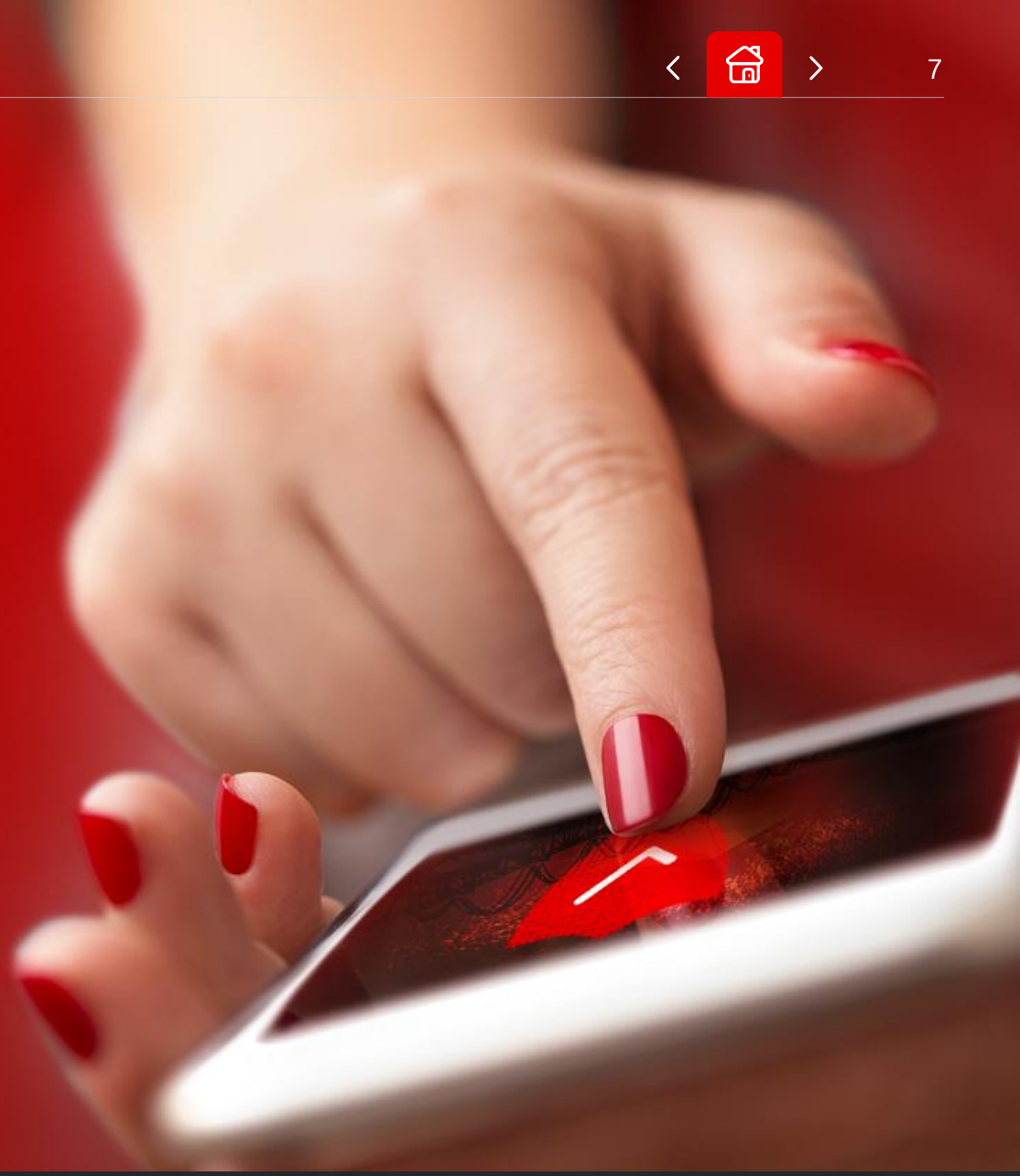
Ist Vodafone Business MDR das Richtige für Ihr Unternehmen?

Sie nutzen EDR-, Cloud-, Netzwerk- oder Identitäts-Lösungen? Von uns oder anderen Anbietern? Unseren MDR-Service können Sie einfach integrieren. Durch dauerhafte Überwachung machen wir Ihr Unternehmen sicherer.

Wir helfen Ihnen, Vorschriften einzuhalten. Und wir beraten Sie. So sind Sie heute sicher und bereit für morgen.

Lassen Sie uns sprechen.

Beratung anfordern



vodafone business