

Vodafone Business Managed Detection and Response Standard

Leitfaden für Kund:innen



Ihr Start mit dem Vodafone Business Security Service

Sie haben Vodafone Business Managed Detection and Response bei Ihrer Ansprechperson im Vertrieb bestellt.

1

Sie bekommen Ihr persönliches Angebot von uns. Bitte akzeptieren Sie die nötigen AGBs. Sie unterschreiben den Vertrag dann mit DocuSign. So bekommen wir den unterschriebenen Vertrag automatisch zurück.

2

Unser lokales Vertriebsteam gibt Ihre Bestellung im Marketplace auf. Danach bekommen Sie eine Willkommens-E-Mail. Darin finden Sie alle Infos zu den nächsten Schritten.



Willkommens-E-Mail

3

**Sie bekommen eine
Willkommens-E-Mail
von uns.
Darin erklären wir Ihnen,
wie Sie Ihren neuen
Service nutzen.**



Betreff: Auftragsbestätigung - Starten Sie mit Ihrem neuen Vodafone Business Managed Detection and Response Service

Vielen Dank, dass Sie sich für **Vodafone Business Managed Detection and Response Service** entschieden haben!

Mehr Infos zu Ihrem Service finden Sie hier: [Kunden-Leitfaden für Vodafone Business Managed Detection and Response](#)

Starten Sie jetzt mit diesen 4 Schritten:

1. Beim Vodafone Business CyberHub registrieren

Sie bekommen von uns eine E-Mail mit dem Betreff „**Vodafone Firmenkundenportal | Einladung / Invitation**“. Öffnen Sie diese E-Mail und registrieren Sie sich mit dem Link in der E-Mail im CyberHub. Bestätigen Sie danach bitte Ihre Anmeldung.

Im CyberHub bekommen Sie alle Infos zu Ihren neuen Services. Hier erstellen Sie Service Requests und bekommen Reportings und Insights zu möglichen Bedrohungen. Außerdem sehen Sie Ihre allgemeine Cyber-Risikolage.

Sie haben nach 3 Tagen noch keine E-Mail bekommen?

Dann melden Sie sich bitte bei uns: vbsoc_support@vodafone.com.

Sie haben schon ein CyberHub-Konto?

Ihr Unternehmen nutzt schon andere Security Services gegen Cyber-Bedrohungen von uns? Sie brauchen sich dann nicht nochmal zu registrieren. CyberHub führt alle zusammen. Unter **Meine Services** finden Sie jetzt auch den Eintrag zu Ihrem neuen Service **Managed Detection & Response**.

Die E-Mail mit dem Betreff „**Vodafone Firmenkundenportal | Einladung / Invitation**“ bekommen Sie dann nicht.

2. Anmelden und Start des Onboardings

Zuerst brauchen wir Infos zu Ihrem aktuellen Setup. Das Vodafone Business Customer SOC Team meldet sich bei Ihnen, um den Kick-Off-Call für das Onboarding zu organisieren. In dem Termin bespricht das Team die nächsten Schritte mit Ihnen. Zusammen planen Sie die weiteren Termine für das Onboarding.

Melden Sie sich mit Ihren Zugangsdaten beim CyberHub an.

Füllen Sie bitte das Formular unter dem Produkt **Managed Detection & Response** im CyberHub aus.

Sie haben Fragen zu dem Formular? Melden Sie sich über unser Self-Service-Portal: <https://cyberhub.vodafone.de>.

Wenn unsere Technik-Teams Fragen haben, melden wir uns bei Ihnen. Achten Sie auf Benachrichtigungen im CyberHub und auf E-Mails vom SOC-Team.

3. Bestätigung der Aktivierung des Services

Wir haben alle Infos von Ihnen bekommen? Dann testen wir die Einrichtung. Wenn alles funktioniert und der Service live gehen kann, meldet sich das Team bei Ihnen.

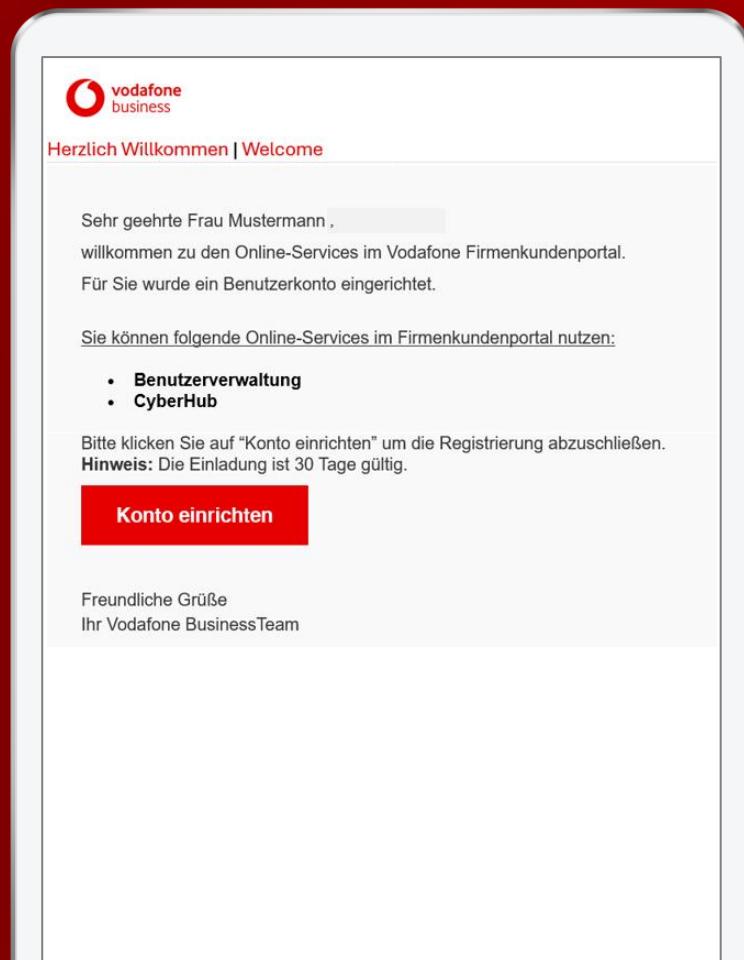
Schließen Sie dann bitte die Aktivierung ab. Das geht in unserem Self-Service-Portal: <https://cyberhub.vodafone.de>. Sobald Sie die Aktivierung bestätigt haben, können Sie den Service nutzen.

Sie haben noch Fragen? Erstellen Sie einfach ein Ticket im CyberHub. Dann melden wir uns so schnell wie möglich bei Ihnen.

Freundliche Grüße

Ihr Vodafone Business Team





Zugriff auf den Vodafone Business CyberHub

4

Ein paar Tage nach der
Willkommens-E-Mail
bekommen Sie noch eine E-
Mail von uns. Damit können Sie
sich im Vodafone Business
CyberHub registrieren und
anmelden.



Kick-Off-Termin zur Einrichtung

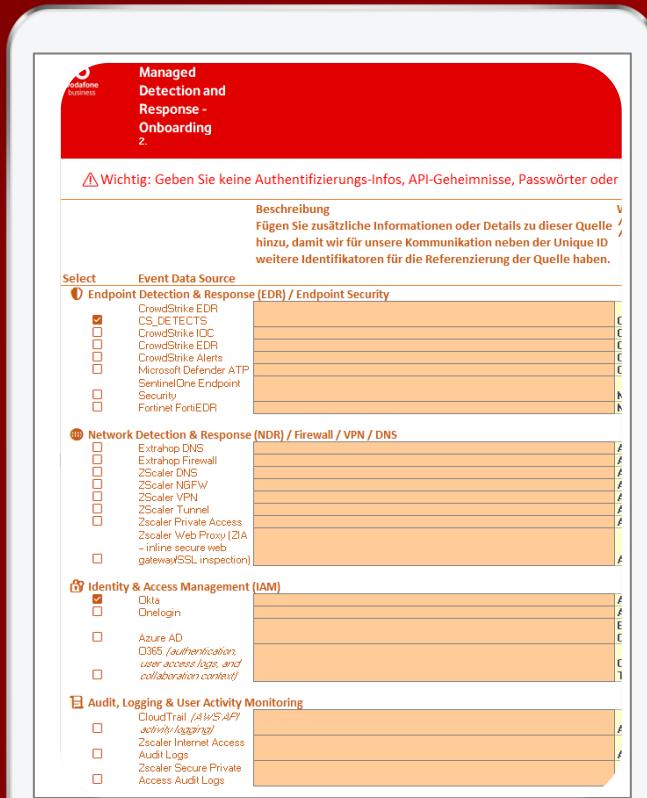
5

Während des Kick-off-Termins erklären wir Ihnen den gesamten Onboarding-Prozess. Dazu gehören auch wichtige Meilensteine, Zeitpläne und Liefergegenstände. Sie wollen Dinge an Ihre Wünsche anpassen? Z.B. individuelle Use Cases nutzen? Oder Unterstützung bei nicht standardisierten Konfigurationen Ihrer Systeme für die Log-Ingestion und Integrationen? Auch das besprechen wir zusammen in diesem Termin.



Onboarding-Formular

6



Managed Detection and Response - Onboarding	
<p>⚠️ Wichtig: Geben Sie keine Authentifizierungs-Infos, API-Geheimnisse, Passwörter oder weitere Identifikatoren für die Referenzierung der Quelle haben.</p>	
Select	Event Data Source
<p>① Endpoint Detection & Response (EDR) / Endpoint Security</p> <input checked="" type="checkbox"/> CrowdStrike EDR <input type="checkbox"/> CS_DETECTS <input type="checkbox"/> CrowdStrike IDC <input type="checkbox"/> CrowdStrike EDR <input type="checkbox"/> CrowdStrike Alerts <input type="checkbox"/> Microsoft Defender ATP <input type="checkbox"/> SentinelOne Endpoint Security <input type="checkbox"/> Fortinet FortiEDR	
<p>② Network Detection & Response (NDR) / Firewall / VPN / DNS</p> <input type="checkbox"/> Extrahop DNS <input type="checkbox"/> Extrahop Firewall <input type="checkbox"/> ZScaler DNS <input type="checkbox"/> ZScaler NGFW <input type="checkbox"/> ZScaler VPN <input type="checkbox"/> ZScaler Tunnel <input type="checkbox"/> ZScaler Private Access <input type="checkbox"/> ZScaler Web Proxy (ZIA - Inline secure web gateway/SSL Inspection)	
<p>③ Identity & Access Management (IAM)</p> <input checked="" type="checkbox"/> Okta <input type="checkbox"/> OneLogin <input type="checkbox"/> Azure AD <small>(Authentication, user access logs, and collaboration context)</small>	
<p>④ Audit, Logging & User Activity Monitoring</p> <input type="checkbox"/> CloudTrail (AWS API activity logs) <input type="checkbox"/> Zscaler Internet Access <input type="checkbox"/> Audit Logs <input type="checkbox"/> Zscaler Secure Private Access Audit Logs	

Sie starten das Onboarding über den CyberHub. Laden Sie dazu das Onboarding-Formular herunter und füllen Sie es aus. Das Dokument dafür finden Sie im CyberHub – unter dem Produkt Managed Detection and Response. Sie brauchen Hilfe beim Ausfüllen des Onboarding-Formulars? Wir helfen Ihnen gerne.

Tragen Sie diese Daten bitte in das Formular ein:

- Kundendaten
- Datenquellen für die Log-Ingestion
- Liste kritischer Assets

Über den CyberHub können Sie immer den Onboarding-Status prüfen.

Sie haben das Formular ausgefüllt? Dann klicken Sie bitte auf „Abschicken“. Sie bekommen eine automatisierte Antwort – sobald unsere Vodafone Security-Expert:innen das Formular bekommen haben.



Abschluss Onboarding

Wir haben noch Fragen? Dann melden wir uns. Das machen wir über das Onboarding-Ticket oder per Telefon.

7

Sie haben noch Fragen? Dann antworten Sie einfach auf das Onboarding-Ticket im Vodafone Business CyberHub.

8

Unsere Vodafone Security-Expert:innen melden sich bei Ihnen – sobald das Onboarding abgeschlossen ist. Sie bekommen einen Bericht – mit allen Maßnahmen und Sicherheitsanpassungen.



Managed Detection and Response

Zusammenfassung & Übersicht

- 1** Sie bekommen Ihr persönliches Angebot von uns. Den Vertrag unterschreiben Sie mit DocuSign.
- 2** Die Bestellung läuft über den Marketplace. Das übernehmen wir.
- 3** Sie bekommen eine Willkommens-E-Mail von uns. Darin finden Sie alle Infos für Ihren neuen Service.
- 4** Sie registrieren sich im Vodafone Business CyberHub. Dort verwalten Sie den Service und die Kommunikation mit Vodafone Business.
- 5** Zusammen stimmen wir einen Kick-off-Termin für die Einrichtung ab. Dort planen wir zusammen die Konfiguration für die Log-Ingestion und Integration Ihrer Systeme – Schritt für Schritt.
- 6** Sie füllen das Onboarding-Formular aus. Gehen Sie dafür im CyberHub auf das Produkt Managed Detection and Response. Dort finden Sie das Formular.

- 7** Wir melden uns, wenn wir Fragen haben. Sie haben noch Fragen? Dann melden Sie sich bitte über das Onboarding-Ticket.
- 8** Sie bekommen eine Info, sobald Sie den Onboarding-Prozess abgeschlossen haben – inklusive Abschlussbericht.





vodafone
business

Together we can