SOPHOS

Vertriebs- und technische FAQs – Sophos Emergency Incident Response

Externe FAQs

Allgemeiner Überblick

Was ist Emergency Incident Response?
Sophos Emergency Incident Response bietet Soforthilfe bei Cyberangriffen, ergreift schnelle Maßnahmen zum Bewerten, Eindämmen, Analysieren und Bereinigen des Vorfalls und gibt Empfehlungen für Korrekturmaßnahmen. Dank jahrelanger Erfahrung und Expertise in verschiedenen Bereichen können unsere Experten akute Bedrohungen schnell priorisieren, eindämmen und beseitigen, bevor weiterer Schaden entsteht.

Mithilfe von Emergency Incident Response können Sie auch ermitteln, ob in Ihrem Unternehmen/Ihrer Organisation ein Sicherheitsvorfall stattgefunden hat, und ggf. das Ausmaß dieses Vorfalls analysieren. Der Service bietet eine Reihe von Analyseaktivitäten an, u. a. Ursachenermittlung von Vorfällen, Compromise Assessments, um festzustellen, ob schädliches Verhalten vorliegt, Threat Hunting und Sammeln von Threat Intelligence sowie Unterstützung bei Lösegeldverhandlungen.

An wen richtet sich Emergency Incident Response?
An alle Unternehmen und Organisationen, die von einem akuten Sicherheitsvorfall betroffen sind, vor Kurzem angegriffen wurden und weitere Analysen durchführen möchten, oder verdächtige Aktivitäten beobachtet haben, die untersucht werden müssen, um zu ermitteln, ob sie eine Bedrohung darstellen.

Muss ich Kunde von Sophos sein, um Emergency Incident Response zu erwerben?
Nein. Emergency Incident Response steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung.

Ich bin von einem aktiven Sicherheitsvorfall betroffen. Was tue ich als Nächstes?
Kontaktieren Sie unsere Incident-Response-Experten jederzeit über die Rufnummer für Ihre Region:

- Deutschland: +49 61171186766
- Österreich: +43 73265575520
- Schweiz: +41 445152286
- Australien: +61 272084454
- Kanada: +1 7785897255
- Frankreich: +33 186539880
- Italien: +39 02 94752 897
- Großbritannien und Nordirland: +44 1235635329
- USA: +1 4087461064

Kontaktieren Sie uns per E-Mail unter EmergencyIR@sophos.com.

Wird Emergency Incident Response remote oder vor Ort bereitgestellt?
Es stehen sowohl Remote- als auch Vor-Ort-Optionen zur Verfügung.

Wie schnell reagiert der Emergency Incident Response Service?
Das Onboarding der meisten Kunden erfolgt binnen zwei Stunden und die Triage ist in der Regel nach 48 Stunden abgeschlossen. Da der Service vollständig remote bereitgestellt werden kann, können bereits wenige Stunden nach Kontaktaufnahme mit Sophos Reaktionsmaßnahmen ergriffen werden.

Wie schnell können Sie mit dem Onboarding beginnen?
Das Emergency Incident Response Team kann mit dem Onboarding-Prozess und ersten Analysen beginnen, sobald Sie Ihre Genehmigung erteilt haben.

Wie läuft ein Einsatz von Emergency Incident Response ab?
Nachdem Sie den Service-Vertrag akzeptiert haben, führen wir ein telefonisches Erstgespräch durch. Auf Wunsch können wir Sie auch per E-Mail kontaktieren. Die Analyse beginnt, sobald wir verstehen, welche Ziele Sie durch unsere Beauftragung verfolgen möchten.

Im Rahmen von Emergency Incident Response können wir verschiedene Kategorien von Dienstleistungen anbieten. Beim Erstgespräch ermitteln wir gemeinsam mit Ihnen die erforderlichen Kategorien und die voraussichtlich erforderliche Anzahl von Arbeitsstunden.

Zu den Schwerpunktkategorien gehören Projekt-Management, Incident Response, digitale Forensik, Compromise Assessment, Threat Hunting, Threat Intelligence und -Bedrohungsforschung, Lösegeldverhandlungen, Projektbericht, Vor-Ort-Support (falls zutreffend), Business Email Compromise und Software-Bereitstellung.

In welchen Sprachen wird Emergency Incident Response angeboten?
Derzeit wird der Service auf Englisch und Japanisch angeboten. Sie müssen über ausreichende Englisch- oder Japanischkenntnisse verfügen.

Kann Sophos mit oder anstelle von Data Forensic Incident Response Services (DFIR) eingesetzt werden?
Emergency Incident Response ist ein DFIR-Service. Es ist nicht erforderlich, ein separates Sicherheitsunternehmen für DFIR zu beauftragen, da der Leistungsumfang, der im Rahmen von Emergency Incident Response erbracht wird, digitale Forensik einschließen kann.

Muss ich Sophos-Technologien auf meinen Endpoints installieren?
Nein, Emergency Incident Response kann mit Sophos XDR bereitgestellt werden, oder wir können neben Ihrer bestehenden Lösung den Sophos XDR Sensor implementieren. Über beide Optionen können wir den Vorfall schnell analysieren.

Das Emergency Incident Response Team kann schon vor Abschluss der Bereitstellung Maßnahmen zum Eindämmen und Beseitigen der Bedrohung ergreifen. Das Team nutzt alle verfügbaren Daten und greift auf Tools zur Unterstützung der Reaktionsmaßnahmen zurück.

Wie wird der Preis berechnet?
Sophos schätzt anhand von Sondierungsfragen, wie viele Stunden zur Reaktion auf den Vorfall benötigt werden. Sie zahlen nur für die tatsächlich genutzten Stunden.

Fallen zusätzliche Kosten an?
Sollte ein Vor-Ort-Einsatz erforderlich sein, werden Ihnen die Reisekosten in Rechnung gestellt.

Kann Emergency Incident Response in nur einem Segment unserer Umgebung implementiert werden oder muss die Implementierung in unserer gesamten Umgebung erfolgen?
In bestimmten Situationen kann Emergency Incident Response auf ein Segment Ihrer Umgebung angewendet werden. Ein Emergency Incident Response Spezialist kann Ihnen im Rahmen der Projektplanung weitere Einzelheiten nennen.

Kann Sophos mit einem Vermittler (z. B. Anwaltskanzlei) zusammenarbeiten, der den Vertrag im Auftrag meines Unternehmens/meiner Organisation abschließt?
Ja. Die Arbeit mit einem Vermittler ist möglich.

Kann Sophos feststellen, welche Dateien beim Angriff exfiltriert/gestohlen wurden?
Im Rahmen des Emergency Incident Response Service unternehmen wir alle Anstrengungen, um festzustellen, ob, und wenn ja, welche Dateien im Rahmen eines Angriffs exfiltriert wurden. Wir können jedoch keine lückenlosen Informationen über Exfiltrationen garantieren, da diese Erkenntnisse von den im Rahmen der Analyse verfügbaren Daten abhängig sind.

Entschlüsselt Sophos Ransomware für mich?
Nein. Diese Leistung ist im Emergency Incident Response Service nicht enthalten.

Hilft Sophos mir, Lösegeld-Zahlungen auszuhandeln oder abzuwickeln?
Emergency Incident Response umfasst Expertenverhandlungen mit Bedrohungsakteuren. Allerdings Sophos leistet Sophos keine aktive Unterstützung bei Lösegeldzahlungen, kann jedoch bei Bedarf Dritte empfehlen und mit ihnen zusammenarbeiten.

2025-06-03 (WP-NP)

SOPHOS