TeamCom
Cloud- und Rechenzentrumslösungen

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

Leistungsbeschreibung – Security Operation Center (SOC)
Stand: Januar 2026

Diese Leistungsbeschreibung definiert die Art, den Umfang und die Rahmenbedingungen der von der TeamCom Goch GmbH angebotenen SOCServices. Sie enthält eine Übersicht über die verfügbaren Leistungspakete, beschreibt deren Grenzen und legt die Mitwirkungspflichten des Auftraggebers fest. Die Beschreibung ist Bestandteil des Vertragsverhältnisses im B2B Bereich und soll die angebotenen Leistungen transparent darstellen.

---

01 Hinweise zu Sicherheit, Leistungsumfang und Haftung

Obwohl das SOC auf marktüblichen Technologien basiert und mit größtmöglicher Sorgfalt betrieben wird, kann die TeamCom Goch GmbH keine Garantie, Zusicherung oder Gewähr für die vollständige Sicherheit der Systeme des Auftraggebers übernehmen.

Ziel der SOC-Leistungen ist es, sicherheitsrelevante Ereignisse zu erkennen, zu analysieren und einzuordnen. Sie dienen nicht der vollständigen Prävention, Abwehr oder Verhinderung von Cyberangriffen. Selbst bei ordnungsgemäßer Nutzung aller Services bleibt ein Restrisiko bestehen, etwa durch Cyberangriffe, ITSicherheitsvorfälle oder Datenverluste.

Die Leistungen erfolgen nach dem Prinzip des „Best Effort“. Das bedeutet: TeamCom erbringt die Leistungen mit angemessener fachlicher Sorgfalt, ohne bestimmte Ergebnisse oder Sicherheitsniveaus zuzusichern. Es besteht keine Verpflichtung zur lückenlosen Erkennung aller Bedrohungen oder Schwachstellen.

Weder ausdrückliche noch stillschweigende Garantien hinsichtlich Reaktionszeit, Verfügbarkeit oder Wirksamkeit werden übernommen – auch nicht bei kritischen Vorfällen oder innerhalb eines 24/7-Serviceumfangs. Die Haftung für einfache Fahrlässigkeit ist – soweit rechtlich zulässig – ausgeschlossen. Bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) haftet TeamCom lediglich auf den vertragstypischen, vorhersehbaren Schaden. Für grobe Fahrlässigkeit und Vorsatz gelten die gesetzlichen Regelungen.

Diese Leistungsbeschreibung stellt kein Garantieversprechen oder eine Zusicherung bestimmter Ergebnisse dar, sondern beschreibt den organisatorischen und technischen Rahmen der angebotenen Leistungen.

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

02 Überblick über die Leistungen

Je nach gewähltem Paket umfasst das SOC:

- Zentrale Erfassung von sicherheitsrelevanten Ereignissen
- Automatisierte und ggf. manuelle Auswertung eingehender Warnmeldungen
- Einstufung und Priorisierung durch Fachpersonal
- Weiterleitung von Erkenntnissen und ggf. Handlungsempfehlungen
- Optional: Durchführung standardisierter Sofortmaßnahmen nach Playbooks

Die Überwachung beschränkt sich auf Systeme, die technisch angebunden und durch TeamCom freigegeben wurden. Dazu zählen insbesondere:

- Endgeräte mit freigegebener Schutzsoftware
- Microsoft-365-Dienste
- Firewalls freigegebener Hersteller

Reaktionszeiten & SLA

Es bestehen keine verbindlichen Service-Level-Agreements. Begriffe wie „sofort“, „proaktiv“, „zeitnah“ oder „24/7“ beschreiben rein organisatorische Ziele und begründen keine einklagbaren Leistungen – auch nicht durch Paketnamen oder Funktionsbeschreibungen.

Klassifikation von Sicherheitsereignissen

Sicherheitsereignisse werden nach fachlichem Ermessen wie folgt klassifiziert:

- low/niedrig: Es ist kein direktes Handeln erforderlich. Eine Prüfung und oder Behebung kann zu gegebener Zeit erfolgen
- Medium: Es ist ein zeitnahes Handeln erforderlich damit eine Warnmeldung nicht zu einem Sicherheitsvorfall in der Zukunft führen kann
- High/Hoch: Es ist ein sehr zeitnahes Handeln erforderlich, da eine mögliche Bedrohung für die Netzwerksicherheit besteht
- Kritisch: Es ist ein sofortiges Handeln erforderlich, da eine Bedrohung für die Netzwerksicherheit besteht und Sofortmaßnahmen ergriffen werden sollten

Die Einstufung liegt ausschließlich im Ermessen des SOC-Teams. Der Auftraggeber hat keinen Anspruch auf Mitsprache der Bewertung.

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

03 Beschreibung der Leistungspakete

3.1 SOC-Paket 1

SOC-Paket 1 umfasst die zentrale Erfassung, Übermittlung und Auswertung sicherheitsrelevanter Daten aus definierten IT-Systemen des Auftraggebers. Die Daten werden automatisiert über vorab geprüfte Schutzmechanismen und Technologien an die Systeme des Auftragnehmers übertragen. Das Paket bietet eine kontinuierliche Sichtbarkeit sicherheitsrelevanter Ereignisse, jedoch keine aktive manuelle Analyse oder Reaktion durch den Auftragnehmer.

Die Überwachung erfolgt auf Basis der eingebundenen IT-Systeme des Auftraggebers.

Die Überprüfung dient der Erkennung unautorisierter Zugriffe, ungewöhnlicher Aktivitäten und möglicher Sicherheitslücken. Eine inkludierte aktive Bearbeitung von Sicherheitsvorfällen erfolgt im Rahmen dieses Pakets nicht. Gesammelte Informationen und deren Einstufung der Kritikalität werden in einem von TeamCom ausgewählten Format an den Kunden übermittelt und sichtbar gemacht. Hierbei gilt folgender Ablauf:

a. Zentrale Sammlung von Log-Daten und Ereignissen sämtlicher angebundener Systeme
b. Automatisierte Analyse mittels vordefinierter Erkennungsrichtlinien
c. Identifikation potenzieller Anomalien und Einstufung durch das System
d. Bereitstellung automatisierter Meldungen in einem Dashboard bzw. Datei gestaffelt nach Kritikalität

Die bereitgestellten Warnmeldungen sind durch den Auftraggeber für seine Systeme zu interpretieren und es gilt eigenständig Maßnahmen zu ergreifen oder die Maßnahmenumsetzung separat bei TeamCom zu beauftragen. Eine manuelle Nachprüfung durch SOC-Analysten ist nicht Bestandteil dieses Pakets. Zur Sammlung der Informationen von integrierten Systemen stellt der Auftragnehmer auf Endpunkten eine Inventarisierungssoftware sowie einer zum SOC zugehörigen Software bereit. Für die Installation der Softwarelösungen ist der Auftraggeber verantwortlich, sofern nicht anderweitig vereinbart oder separat beauftragt. Beide Softwarelösungen sind Voraussetzung für das SOC (siehe 5.) Im Rahmen des Paketes erfolgt eine wöchentliche automatisierte Datenleck Prüfung der Auftraggeber-E-Mail Domain im Darknet. Hierbei wird ausschließlich die Haupt-E-Mail Domain des Auftraggebers und alle damit auffindbaren E-Mail-Adressen geprüft. Kompromittierte bzw. aufgefundene Zugangsdaten werden an den Auftraggeber per E-Mail gemeldet oder in seinem Dashboard dargestellt.

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

Abgrenzung
Im SOC-Paket 1 nicht enthalten sind insbesondere:

a. manuelle Analysen oder Bewertungen durch SOC-Analysten
b. proaktive Reaktion auf sicherheitsrelevante Ereignisse
c. Durchführung von Sofortmaßnahmen

Die Buchung solcher Leistungen ist nur im Rahmen der Pakete 2 oder 3 sowie optional als zusätzliche Incident-Bearbeitung nach Stundensätzen zu buchbar.

3.2 SOC-Paket 2

Das SOC Paket 2 umfasst alle Leistungen aus Paket 1 sowie eine aktive sicherheitsrelevante Analyse während der TeamCom Supportzeiten (Mo-Fr 9-17 Uhr). Das SOC prüft eingehende sicherheitsrelevante Warnmeldungen manuell, stuft diese ein und leitet entsprechende Handlungsempfehlungen an den Auftraggeber bzw. Verantwortliche.

Leistungsbestandteil ist somit die manuelle Ereignisprüfung und Priorisierung sowie die Analyse eingehender Warnmeldungen durch geschulte SOC-Analysten während der TeamCom Supportzeiten. Ebenso die anschließende Klassifizierung von Ereignissen gemäß Kritikalitätsstufen (niedrig, mittel, hoch) und die Priorisierung sicherheitsrelevanter Vorfälle sowie die Überprüfung möglicher Kompromittierungsindikatoren (IoCs) mit Meldung an den Auftraggeber.

Incident Response für Ereignisse mit Kritikalität „hoch“, „niedrig“ & „mittel“ im Rahmen des Pakets:

a. Analyse der Ereignisse und Überführung dieser ins Dashboard bzw. Datei
b. ggf. Ausgabe eines Handlungsvorschlags an die vom Auftraggeber benannten Ansprechpartner/Verantwortlichen

Eine Umsetzung der Maßnahmen in der IT-Umgebung des Auftraggebers erfolgt nicht im Rahmen des Paketumfangs und ist nach Stundensätzen zu buchbar.

Incident Response für Ereignisse mit Kritikalität „kritisch“ im Rahmen des Pakets:

a. Analyse der Ereignisse und Überführung dieser ins Dashboard bzw. Datei
b. Kontaktaufnahme mit Verantwortlichen beim Auftraggeber und Handlungsempfehlungen zur Eindämmung oder Behebung

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

Zur Bearbeitung von kritischen Sicherheitsereignissen führt der Auftragnehmer ausschließlich vordefinierte Maßnahmen gemäß standardisierter Playbooks durch, beispielsweise exemplarisch genannt:

a. Sperrung von Benutzerkonten
b. Anpassung von Firewall- oder Filterregeln
c. Unterbindung schädlicher Prozesse bspw. durch Abschalten von Systemen

Maßnahmen außerhalb der Playbooks sowie aktive Änderungen an Systemen, Netzwerken oder Konfigurationen sind nicht Bestandteil des Leistungsumfangs und können mit separater Beauftragung von TeamCom durchgeführt werden. Vor dem Ergreifen der Maßnahme informiert der Auftragnehmer einen Verantwortlichen des Auftraggebers per E-Mail oder telefonisch über die Maßnahmen.

Welche Systeme & Dienste von TeamCom nach Standard Playbooks verwaltet/isoliert/gesperrt werden dürfen wird im Rahmen des Onboardings mit dem Auftraggeber besprochen und in einer Freigabe Matrix festgehalten.

Abgrenzung
Im SOC-Paket 2 nicht enthalten sind:

a. Maßnahmen außerhalb der definierten Servicezeiten
b. Eingriffe in Systeme oder Netzwerke des Auftraggebers außerhalb kritischer Incidents
c. Moderation oder Kommunikation mit Dritten
d. Maßnahmen außerhalb der Standard-Playbooks

Hinweis: Playbook-Maßnahmen sind begrenzte, standardisierte Reaktionen. Sie ersetzen keine umfassenden Notfallprozesse des Kunden und beinhalten keine generalistischen oder konzeptionellen Veränderungen der IT-Architektur.

Nicht enthalten:
- Eingriffe außerhalb der Playbooks oder Supportzeiten
- Bearbeitung von Incidents mit niedriger oder mittlerer Kritikalität
- Systemwiederherstellungen oder Datenrettung

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

3.3 SOC-Paket 3

Zusätzlich zu Paket 2 können folgende Optionen gesamtheitlich oder einzeln zugebucht werden:

- Erweiterte Erreichbarkeit (24/7 inkl. Feiertage in NRW)
- inkludierte Bearbeitung aller SOC-Vorfälle / Sicherheitsereignisse (Fair Use gilt)
- Wöchentliche Review-Meetings (zu je 30 Minuten auf einer von Team-IT definierten Plattform)
- Zuweisung eines festen SOC-Kontakts (werktags, keine Exklusivität)
- KI-gestützte Endpoint-Isolation bei klar erkannten Bedrohungen

Hinweis: Die KI-Funktionen dienen der automatisierten Unterstützung. Eine Garantie auf korrekte Entscheidungen besteht nicht.

Nicht enthalten:
- Garantie für KI-Erkennung
- Systemwiederherstellungen
- Exklusive Ressourcenzuteilung

Ein Paketwechsel ist jeweils zum Monatsende mit fünf Werktagen Vorlauf möglich.

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

04 Zubuchbare Optionen

4.1 Firewall-Integration
Ergänzend zu den in das Security Operation Center eingebundenen Endpunkten können freigegebene Firewalls in das Security Operation Center angebunden werden, um die dortigen Logs zu Sicherheitswarnungen und Benachrichtigungen zu Sicherheitsereignissen im SOC zu verarbeiten.

4.2 Notfallrufnummer (Wochenende)
- Verfügbarkeit Fr 17:00 – So 24:00 Uhr für Vorfälle höchster Kritikalität
- Ersteinschätzung durch Analysten mit Handlungsempfehlung
- Maßnahmenumsetzung durch das SOC ist weiterhin kostenpflichtig und separat berechnet

05 Technische Voraussetzungen & Mitwirkung

a. Unabhängig der Benutzeranzahl des Auftraggebers wird eine Grundgebühr pro SOC-Instanz (Umgebung) fällig.
b. Beim Einsatz von Microsoft 365 ist eine Anbindung der Umgebung zwingend erforderlich.
c. Der Auftraggeber muss mindestens eine Mobilnummer einer Person der Geschäftsleitung bereitstellen, um die Erreichbarkeit im Notfall sicherzustellen (gilt insbesondere für Pakete 2 und 3).
d. Wird auf Endgeräten oder Servern bereits eine RMM-Software eines Drittanbieters eingesetzt, trägt der Dritte die Verantwortung für den Manipulationsschutz der SOC-Dienste. Ebenso ist der Dritte bzw. der Auftraggeber dazu verpflichtet dafür zu sorgen, dass die angebundenen Endpunkte stets aktuell und vollständig mit den SOC-Diensten versorgt sind.

Adresse
Daimler Str. 44,
47574 Goch

E-Mail
vertrieb@team-it-group.de

Telefon
+49 2823 9440 - 115

06 Datenschutz & Datenverarbeitung

Die Verarbeitung erfolgt ausschließlich DSGVO-konform auf Servern in Deutschland. Eine Datenweitergabe erfolgt nur bei gesetzlicher Pflicht. Ereignisdaten werden maximal 90 Tage gespeichert und danach automatisch gelöscht, sofern keine abweichende Regelung besteht.

Zur Erfüllung aller benannten Leistungen ist es TeamCom freigestellt die Leistungen selbst zu erbringen oder ein Unternehmen innerhalb der Team-IT Group mit der Erfüllung zu beauftragen bzw. den Auftrag zu vermitteln. Für alle beteiligten Unternehmen gelten die Erläuterungen aus Punkt 1.

07 Fair Use Policy

Die Nutzung der Leistungen unterliegt einer Fair-Use-Regelung. Bei deutlicher Überschreitung (z. B. mehr als das Dreifache des Paketniveaus) behält sich TeamCom vor, Leistungen anzupassen, einzuschränken oder gesondert zu berechnen.

08 Exklusivität der Administration

Das SOC wird ausschließlich durch TeamCom administriert. Der Kunde erhält keinen Zugriff auf interne Systeme oder Administrationsfunktionen.

09 Ergänzende Regelungen

Es gelten die AGB der TeamCom Goch GmbH. Bei Widersprüchen gilt folgende Reihenfolge: 1. Individuelles Angebot 2. Allgemeine Geschäftsbedingungen 3. Diese Leistungsbeschreibung Weitere Abweichungen gelten nur bei schriftlicher Vereinbarung.

Diese Leistungsbeschreibung dient rein informativen Zwecken und stellt keine rechtsverbindliche Zusage oder Garantie dar. Änderungen vorbehalten.