Service Level Agreement

(Leistungsbeschreibung)

CDC Threat Intelligence Service

Code: FS-CDC-TIS
Version: 3.0
Gültig ab 01.01.2025

CANCOM Austria AG // Wienerbergstraße 53 // 1120 Wien // Österreich // T +43 50 822 0 // info@cancom.com
HG Wien FN 178368g // Firmensitz Wien // UID ATU46276408 // InterzeroNr. 155219
Raiffeisenlandesbank Oberösterreich // BIC: RZOOAT2L // IBAN: AT35 3400 0000 0009 7899 // Creditor-ID: AT17ZZZ00000029797
www.cancom.at

Leistungen des Auftragnehmers

Dieses Dokument beschreibt die Serviceleistungen des Servicemoduls, welche im Rahmen des zwischen dem Auftraggeber (AG) und Auftragnehmer (AN) abgeschlossenen Vertrages erbracht wird. Die Verantwortlichkeiten der beschriebenen Leistungen sind auf Basis eines RACI-Modells abgebildet. Begriffserklärungen sowie Kontakt Informationen des Customer Service Center sind unter folgendem *Link* zu finden.

Sofern nichts Gegenteiliges vereinbart ist, gelten standardmäßig folgende Serviceziele: Servicezeit „SNAZ“ (NWH) mit einer Reaktionszeit von 4 Stunden.

CDC Threat Intelligence Service

Das Threat Intelligence Service (TIS) liefert Informationen über die aktuelle Bedrohungslage in Bezug auf Ihr Unternehmen. CDC TI Analysten durchsuchen das Internet, Deep Web, Dark Web, Paste Sites und Code Repositories nach Threats und geleakte Informationen.

Initiale Leistungen	AN	AG
Bestandsaufnahme der Assets mit dem Kunden	R/A	C/I
Implementieren des Asset Monitorings	R/A	C/I
Hinterlegen der Kontaktdaten der vom Kunden definierten Ansprechpersonen im Service Management System des Auftragnehmers	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Prüfung und Auswertung der gefundenen Daten im Internet, Dark und Deep Web		
Der Auftragnehmer ist beauftragt, eine gründliche Überprüfung und Auswertung von Daten durchzuführen, die im Internet, im Dark Web und im Deep Web gefunden werden. Diese Aufgabe beinhaltet die Untersuchung von Informationen und Inhalten auf verschiedenen Ebenen des Internets, einschließlich öffentlicher Websites, nicht indexierter Bereiche (Dark Web) und schwer zugänglicher Bereiche (Deep Web). Der Fokus liegt dabei auf der Identifizierung, Überprüfung und Analyse von relevanten Informationen, um potenzielle Bedrohungen oder Sicherheitsrisiken zu erkennen. Die Ergebnisse dieser Überprüfung bilden die Grundlage für eine umfassende Bewertung der Datenquellen durch den Auftragnehmer. Diese fundierte Bewertung ermöglicht eine informierte Entscheidungsgrundlage in Bezug auf Sicherheitsaspekte und die Gewinnung von relevanten Informationen. Der Auftragnehmer trägt somit dazu bei, potenzielle Risiken frühzeitig zu identifizieren und eine proaktive Sicherheitsstrategie zu entwickeln.	R/A	C/I
Brand & Credential Monitoring		
Im Rahmen des Brand-, Asset- und Credential-Monitorings erfolgt eine gezielte Suche nach geleakten Informationen, Markennamen und Diskussionen über Unternehmen in verschiedenen Branchen. Der Auftragnehmer sammelt dabei definierte Bedrohungsinformationen bzw. Events aus verschiedenen Threat Intelligence Quellen und führt umfassende Analysen durch. Falls	R/A	C/I

geleakte Informationen oder Bedrohungsszenarien identifiziert werden, informiert der Auftragnehmer den Auftraggeber gemäß zuvor getroffener Kommunikationsvereinbarungen. Die Suche konzentriert sich auf folgende Datenkategorien: • Brand / Asset / Credentials (Benutzer, Passwörter) • Trendanalysen im Zusammenhang mit dem Auftraggeber • Firmennamen und Firmenmarken • Systeminformationen für Schwachstellenanalysen Dieser Prozess ermöglicht es dem Auftraggeber, frühzeitig auf mögliche Bedrohungen und Sicherheitsrisiken zu reagieren und entsprechende Gegenmaßnahmen zu ergreifen.		
Security Reports über Bedrohungen und Risiken		
Der Auftraggeber erhält gemäß den vereinbarten Regelungen regelmäßig einen umfassenden Security Report. Dieser Report bietet in einer Management Summary einen Überblick über die Bedrohungen im Netz, darunter Top Threats mit Risikobewertung sowie detaillierte Informationen zu jeder identifizierten Bedrohung. Zusätzlich enthält der Bericht eingehende technische Details, die Einblicke in die Analyse und Klassifizierung der einzelnen Ereignisse gewähren. Diese umfassende Dokumentation ermöglicht es dem Auftraggeber, die Sicherheit seines Netzwerks besser zu verstehen und gezielte Maßnahmen zur Risikominderung zu ergreifen.	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung von Dokumentationen		
Der Auftraggeber stellt im Rahmen des Threat Intelligence Monitorings die benötigte Dokumentation (Netzwerkplan, IP-Adressen, Services) sowie relevante Informationen (Firmennamen, Domains, Projekte usw.) bereit. Diese Daten sind für die Threat Intelligence Analysten entscheidend, um geleakte Informationen abzugleichen und die aktuelle Bedrohungslage präzise darzustellen.	C/I	R/A
Bereitstellung von notwendiger Ressourcen		
Während des Onboarding Prozesses liegt es in der Verantwortung des Auftraggebers, erforderliche Dokumente auszufüllen, verfügbare IT- und Personalressourcen bereitzustellen (z. B. virtuelle Appliance gemäß den Vorgaben des Auftragnehmers, Microsoft-Lizenzen während der Implementierungsphasen und Betrieb der Services) und aktiv bei der Einrichtung des Fernzugriffs zu unterstützen.	C/I	R/A

Rahmenbedingungen für die Leistungserbringung
Am Ende der Vertragslaufzeit werden alle bereitgestellten Daten gemäß den Vereinbarungen sicher gelöscht.

Nicht enthaltene Leistungen
Prüfung des Netzwerkverkehrs auf Anomalien mittels Signaturen und Reputationsdaten (NSM)
Analyse von Logfiles nicht definierter Systeme von Auftragnehmer
Monitoren und Analysen von Endpoint Aktivitäten (EDR)
Umsetzung der im Security Report empfohlenen Maßnahmen