Service Level Agreement

(Leistungsbeschreibung)

CDC Endpoint Detection Response Service

Code: FS-CDC-EDR
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 Endpoint Detection Response Service

Das Endpoint Detection and Response Service bezieht sich auf die Überwachung von einzelnen Geräten (Endpunkten) in einem Netzwerk. Ziel ist die frühzeitige Erkennung von verdächtigem Verhalten oder Anomalien, um mögliche Sicherheitsverletzungen rechtzeitig zu identifizieren.

Initiale Leistungen	AN	AG
Bestandsaufnahme der bestehenden IT-Infrastruktur und der technischen Services mit dem Kunden	R/A	C/I
Hinterlegen der Kontaktdaten der vom Kunden definierten Ansprechpersonen im Service Management System des Auftragnehmers	R/A	C/I
Definieren, Einrichten und Testen des Zuganges	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Monitoring der Endpoint Aktivitäten und Reaktion auf Sicherheitsvorfälle durch Endpoint Detection and Response		
Das Cyber Defense Center überwacht Server und Clients mithilfe der eingesetzten Endpoint Detection and Response Lösung. Der Auftraggeber installiert auf den Systemen, sofern nicht vom Auftragnehmer verwaltet, einen Agenten, der Änderungen und Artefakte am System aufzeichnet und an eine zentrale Management-Plattform sendet. Die gewonnenen Informationen dienen zur Identifikation von Angriffen durch Indicators of Compromise und zusätzliche Erkennungsmethoden, wodurch Alarme generiert werden. Sobald Alarme auf einem Endpoint auftreten, initiiert ein CDC-Analyst den Analyseprozess. Der Analyst verbindet sich mit dem betroffenen System, analysiert es, sammelt Artefakte und bereichert diese gegebenenfalls mit weiterer Threat Intelligence. Falls weitere CDC-Module beim Auftraggeber vorhanden sind, werden die Informationen korreliert und zusammengeführt, um einen umfassenderen Einblick in die Bedrohungslage zu gewährleisten. Im Zuge der Analyse wird auch dokumentiert, in welche Phase der Cyber Kill-Chain der Angriff einzuordnen ist, basierend auf dem MITRE Attack Framework. Dieses Modul ermöglicht eine direkte Nachverfolgung der Bedrohungen für Endgeräte, identifiziert, welche Daten von Angreifern oder Schadsoftware abgegriffen, verändert oder erstellt wurden, und welche Systeme in einen Data Breach involviert waren. Des Weiteren kann die sogenannte Ost-West-Kommunikation (Lateral Movement) von Angreifern erkannt werden – die Kommunikation eines Angreifers innerhalb des kompromittierten Netzwerks.	R/A	C/I

Wenn ein System als kompromittiert identifiziert wird, besteht die Möglichkeit, es in Quarantäne zu versetzen und nur noch mit speziellen Analyse-Systemen kommunizieren zu lassen. Dies erfolgt unabhängig davon, ob sich das kompromittierte System gerade im öffentlichen Internet oder im Unternehmensnetzwerk befindet. Es werden also ausschließlich Daten vom Endpoint analysiert - keine Netzwerk- oder Log Daten. <u>Bewertung von Vorfällen</u> Im Rahmen der Analyse werden relevante Alarme, Indikatoren und Artefakte gesammelt, die mit einem Vorfall in Verbindung stehen. Der Vorfall wird vom Analysten manuell überprüft und bewertet. Bei der Bewertung kann es sich entweder um ein Fehlalarm (False Positive) oder um einen echten Vorfall (True Positive) handeln. Fehlalarm (False Positive): Wenn es sich bei dem genauer untersuchten Vorfall um einen Fehlalarm handelt, wird der Vorfall entsprechend im CDC-Portal dokumentiert und als Fehlalarm klassifiziert. In diesem Fall erfolgt keine Rückmeldung an den Auftraggeber. Fehlalarme werden im CDC-Portal und im monatlichen Bericht als solche aufgeführt. Echter Vorfall ohne Auswirkungen (True Positive – NI): Handelt es sich bei dem genauer untersuchten Vorfall um einen echten Vorfall ohne Auswirkungen (NI), wird der Vorfall im CDC-Portal dokumentiert und als echter Vorfall ohne Auswirkungen klassifiziert. Die Klassifizierung als echter Vorfall ohne Auswirkungen erfolgt nach Rücksprache mit dem Auftraggeber. Diese echten Vorfälle ohne Auswirkungen werden im CDC-Portal und im monatlichen Bericht aufgeführt. Beispiele hierfür sind Audits, erfolglose Exploits, Phishing ohne Klick auf die URL, etc. Echter Vorfall mit Auswirkungen (True Positive - WI): Handelt es sich bei dem Vorfall um einen echten Vorfall, eruiert der Analyst den Angriffsvektor und die Bedingungen, unter denen der Angriff auf dem Endpunkt wirksam wurde. Es wird auch analysiert, welche Aktionen der Angreifer auf dem System durchführen konnte und ob es zu einer Verbreitung auf andere Systeme gekommen ist. Anschließend erfolgt eine Klassifizierung des Vorfalls nach seiner Risikoklasse (siehe Klassifizierung von Vorfällen) und die Ausarbeitung eines Maßnahmenplans durch den Analysten. Der Vorfall gilt fortan als verifizierter echter Vorfall. <u>Klassifizierung von Vorfällen</u> Vorfälle werden im Rahmen der Analyse nach Risikoklasse kategorisiert. Die Risikoklassen sind wie folgt definiert: Major: Ein Major-Vorfall weist klare Indikatoren auf, die auf ein kompromittiertes System hinweisen, insbesondere: • Kommunikation mit Command & Control (C&C) • Nachweise für die Exfiltration von Daten • Nachweise für die Ausführung von Schadsoftware • Nachweise für einen Angreifer, der ein System übernommen hat • Nachweise von lateralen Bewegungen (Lateral Movement) • Nachweise für erfolgreiche 3rd Party-Logins Minor: Das System ist nicht eindeutig kompromittiert, zeigt jedoch verdächtiges Verhalten, insbesondere: • Heruntergeladene bösartige Software ohne Nachweis der Ausführung • Ausgeführtes Exploit ohne Erfolgsnachweis • Verdächtiges Verhalten im Netzwerkverkehr (ungewöhnliche Anzahl von Verbindungen, ungewöhnliche Ports usw.) • Zugang zu verdächtigen Domänen • AV-Blockierung auf einem Low-Value-Host		

Informational: Das System ist nicht gefährdet, aber bestimmte Maßnahmen sollten ergriffen werden, um den Gesamtstatus der IT-Umgebung zu optimieren. Dies könnte beispielsweise die Aktualisierung von Funktionalitäten, die Deaktivierung des Server-Headers, Konfigurationen oder Optimierungen umfassen.		
Analyse der Daten, Deklaration von erkannten, Sicherheitrelevanten Bedrohungen		
Gemäß der getroffenen Vereinbarung erhält der Auftraggeber einen monatlichen Security Report. Dieser beinhaltet in einer Management Summary eine Übersicht über Netzwerkbedrohungen, einschließlich Top Threats mit Risikobewertung sowie detaillierte Informationen zu spezifischen Bedrohungen. Der Bericht enthält auch technische Details zur Analyse und Klassifizierung der Ereignisse. Im Rahmen des Berichts werden kurz- und langfristige Maßnahmen entwickelt, um zukünftige Bedrohungen zu verhindern oder zumindest zu erschweren. Diese Empfehlungen werden dem Auftraggeber vorgestellt und in monatlichen Service Meetings erläutert. Die Umsetzung der empfohlenen Maßnahmen liegt in der Verantwortung des Auftraggebers. Der monatliche Report beinhaltet die Rückmeldung der sofern definierten Key Performance Indicators (KPIs) an den Auftraggeber, darunter die Anzahl der Hosts im EDR Service, die Anzahl der Tickets/Incidents mit Trendanalyse, gemeldete Incidents nach Risikoklasse und die Anzahl an True und False Positives.	R/A	C/I
Security Reports über Bedrohungen und Risiken inklusive Darstellung der erforderlichen Maßnahmen		
Gemäß der getroffenen Vereinbarung erhält der Auftraggeber einen monatlichen Security Report. Dieser beinhaltet in einer Management Summary eine Übersicht über Netzwerkbedrohungen, einschließlich Top Threats mit Risikobewertung sowie detaillierte Informationen zu spezifischen Bedrohungen. Der Bericht enthält auch technische Details zur Analyse und Klassifizierung der Ereignisse. Im Rahmen des Berichts werden kurz- und langfristige Maßnahmen entwickelt, um zukünftige Bedrohungen zu verhindern oder zumindest zu erschweren. Diese Empfehlungen werden dem Auftraggeber vorgestellt und in monatlichen Service Meetings erläutert. Die Umsetzung der empfohlenen Maßnahmen liegt in der Verantwortung des Auftraggebers. Der monatliche Report beinhaltet die Rückmeldung der sofern definierten Key Performance Indicators (KPIs) an den Auftraggeber, darunter die Anzahl der Hosts im EDR Service, die Anzahl der Tickets/Incidents mit Trendanalyse, gemeldete Incidents nach Risikoklasse und die Anzahl an True und False Positives.	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung von Dokumentationen		
Der Auftraggeber stellt im Rahmen des Onboarding Prozesses sämtliche erforderliche Dokumentation (einschließlich Netzwerkplan, IP-Adressen, Servernamen und Services) sowie alle technischen Voraussetzungen bereit.	C/I	R/A
Bereitstellung von notwendiger Hardware / Software		
Der Auftragnehmer stellt dem Auntraggeber ein Webportal zur Verfügung, über das alle relevanten Security Incidents eingesehen werden können. Hierfür ist vom Auftraggeber die Bereitstellung einer virtuellen Maschine erforderlich, da das Portal lokal beim Auftragnehmer gehostet wird. Auch die Bereitstellung von Microsoft-Lizenzen, sofern diese benötigt wrden, während der Implementierungsphasen und des Betriebs der Services sowie die aktive Unterstützung bei der Einrichtung des Fernzugriffs gehören zu den Verantwortlichkeiten des Auftraggebers.	C/I	R/A
Informationen für den Onboarding Prozess		
Während des Onboarding Prozesses obliegt es dem Auftraggeber, notwendige Dokumente auszufüllen und verfügbare IT- und Personalressourcen bereitzustellen	C/I	R/A

Rahmenbedingungen für die Leistungserbringung
Während der gesamten Vertragslaufzeit benötigt der Auftragnehmer kontinuierlichen Zugriff auf die CDC Appliance, wobei der Auftraggeber keinen direkten Zugriff auf die Appliance oder die darauf befindlichen Daten hat. Zum Vertragsende erfolgt seitens des Auftragnehmers die Löschung der Daten auf der CDC Appliance.
Zur effizienten Kommunikation und Koordination werden auftraggeberseitig bis zu fünf Ansprechpartner festgelegt, die als Schnittstelle für den laufenden Betrieb dienen.

Nicht enthaltene Leistungen
Prüfung des Netzwerkverkehrs auf Anomalien mittels Signaturen und Reputationsdaten (NSM)
Analysen und Monitoring von Mobile und IoT/OT Devices
Prüfung und Auswertung der LOGs von unterschiedlichen Systemen um Angriffsmuster und Anomalien zu erkennen
Prüfung und Auswertung anderer Endpoint Software vom Auftraggeber
Umsetzung der im Security Report empfohlenen Maßnahmen
Netzwerkkabel (Standard od. LWL)
Ausrollen der EDR-Agents auf den Endpunkten

CANCOM