



Service Level Agreement (Leistungsbeschreibung) CDC LOG Analysis

Code: FS-CDC-LOG
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 LOG Analysis

Das Log Analysis oder auch SIEM (Security Information and Event Management) ist eine Sicherheitslösung, die in Echtzeit Sicherheitsereignisse überwacht, analysiert und korreliert.

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

Wiederkehrende Leistungen	AN	AG
Auswertung der Logfiles von unterschiedlichen Devices im Netzwerk durch Log Analyse		
Der Auftragnehmer führt die Sammlung und Analyse definierter Logfiles bzw. Events von speziellen Systemen durch. Diese Logfiles werden intensiv analysiert und auf Unregelmäßigkeiten überprüft. Die Daten werden auf unterschiedliche Weisen ausgewertet, darunter fallen Visualisierung und Baselining. Eine Anreicherung der Daten mit Content wie Threat Intelligence Informationen ermöglicht eine präzisere Bewertung der einzelnen Events. Durch diese kontinuierliche Auswertung und Analyse der Logfiles erhält man einen umfassenden Überblick über das gesamte Unternehmen und kann die aktuelle Bedrohungslage vollständig erfassen. Die Log-Analyse bietet die Möglichkeit, ein Unternehmensnetzwerk, das über verschiedene Standorte oder sogar Kontinente verteilt ist, einem zentralen Security Monitoring zu unterziehen. Identifiziert das System kritische Events, erfolgt eine unverzügliche Benachrichtigung des Auftraggebers über vordefinierte Kommunikationswege. Bei Bedarf können daraufhin tiefgehende Analysen durchgeführt werden. Der Auftragnehmer sammelt, normalisiert und korreliert die Logfiles an einem zentralen Punkt. Typischerweise werden Logfiles von verschiedenen Systemen erfasst, darunter Proxyservern, Mailgateways, DNS-Servern, Windows Domain Controllern, Antiviren-Produkten, Firewalls und mehr. Es ist wichtig zu betonen, dass bei der Log-Analyse keine Analyse von Netzwerk- oder	R/A	C/I

Endpoint-Daten erfolgt. Der Fokus liegt ausschließlich auf der Auswertung und Überwachung von systemgenerierten Logfiles und Events. Nutzung des Log-Analyse-Tools durch den Auftraggeber: Der Auftraggeber hat die Möglichkeit, das Log-Analyse-Tool für eigene Auswertungen oder IT-Operationen zu nutzen. Hierbei stehen ihm die im Rahmen des Moduls Log-Analyse gesammelten Daten zur Verfügung. Sollte der Auftraggeber darüber hinaus Daten benötigen, die für den Auftragnehmer nicht relevant sind, besteht die Option, diese zusätzlichen Daten in das Log-Analyse-Tool zu integrieren. Es ist wichtig zu beachten, dass damit verbundene Kosten wie beispielsweise Lizenzgebühren, Hardware oder die Datenanbindung von Geräten nicht im Servicepreis enthalten sind und nach tatsächlichem Aufwand separat in Rechnung gestellt werden. Diese flexible Lösung ermöglicht es dem Auftraggeber, maßgeschneiderte Analysen durchzuführen und das Log-Analyse-Tool nach seinen individuellen Anforderungen zu nutzen.		
Analyse der Daten, Deklaration von erkannten, sicherheitsrelevanten Bedrohungen		
Nach Abschluss der Analyse und Feststellung von Sicherheitsbedrohungen oder -lücken im Netzwerk informiert der Auftragnehmer unverzüglich den Auftraggeber über diese Ergebnisse. Diese transparente Kommunikation ermöglicht es dem Auftraggeber, zeitnah Kenntnis von potenziellen Gefahren zu erhalten und entsprechende Maßnahmen zu ergreifen, um die Sicherheit seines Netzwerks zu gewährleisten.	R/A	C/I
Security Reports über Bedrohungen und Risiken inklusive Darstellung der erforderlichen Maßnahmen		
Gemäß der getroffenen Vereinbarung erhält der Auftraggeber regelmäßige Sicherheitsberichte, die in einer Management Summary einen umfassenden Überblick über die Netzwerkbedrohungen bieten. Diese Berichte enthalten eine Risikobewertung der Top-Bedrohungen sowie detaillierte Informationen zu den Ereignissen, einschließlich technischer Analysen und Klassifizierungen. Zusätzlich zu den Berichten werden kurz- und langfristige Maßnahmen entwickelt, die darauf abzielen, zukünftige Bedrohungen zu verhindern oder zumindest zu erschweren. Diese Maßnahmen werden dem Auftraggeber im Rahmen des Berichts als Empfehlungen präsentiert.	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung von Dokumentationen		
Der Auftraggeber ist verantwortlich für die Bereitstellung sämtlicher Dokumentation, darunter Netzwerkpläne, IP-Adressen, Servernamen und Services, sowie aller technischen Voraussetzungen.	C/I	R/A
Bereitstellung von notwendiger Ressourcen		
Während des Onboarding-Prozesses obliegt es dem Auftraggeber, notwendige Dokumente auszufüllen, verfügbare IT- und Personalressourcen bereitzustellen (z. B. virtuelle Appliance gemäß den Vorgaben des Auftragnehmers, Microsoft-Lizenzen während der Implementierungsphasen und für den Betrieb der Services), aktiv bei der Einrichtung des	C/I	R/A

Fernzugriffs zu unterstützen sowie das Anbinden und Weiterleiten verschiedener LOG-Quellen zu gewährleisten.		
Zugriff auf Webportal		
Der Auftragnehmer stellt dem Auftraggeber ein Webportal zur Verfügung, auf dem alle relevanten Security Incidents eingesehen werden können. Hierfür muss der Auftraggeber dem Auftragnehmer eine virtuelle Maschine bereitstellen, da das Portal lokal beim Auftragnehmer betrieben wird.	C/I	R/A

Rahmenbedingungen für die Leistungserbringung

Während der gesamten Vertragslaufzeit benötigt der Auftragnehmer kontinuierlichen Zugriff auf die Cyber Defense Appliance. Der Auftraggeber hat zu keinem Zeitpunkt Zugriff auf die Appliance oder die darauf befindlichen Daten.
Zur effizienten Kommunikation und Koordination werden auftraggeberseitig bis zu fünf Ansprechpartner festgelegt, die als Schnittstelle für den laufenden Betrieb dienen.
Nach Abschluss der Vertragslaufzeit wird der Auftragnehmer alle Daten auf der Cyber Defense Appliance löschen

Nicht enthaltene Leistungen

Prüfung des Netzwerkverkehrs auf Anomalien mittels Signaturen und Reputationsdaten
Analyse von Logfiles nicht definierter Systeme von Auftragnehmer
Monitoren und Analysen von Endpoint Aktivitäten
Umsetzung der im Security Report empfohlenen Maßnahmen

