Service-bezogene Beschreibung

SOC as a Service

Version 1.3 (08.07.2025)

1. Bezeichnung und Gegenstand des Service

1.1 Gegenstand des Service

Der Service betrifft Leistungen im Bereich „SOC as a Service“.

1.2 Zweck, Umfang und Art des Service

Art und Umfang sowie die ausschließlichen Zwecke der Verarbeitung der Auftragsdaten durch den Auftragnehmer vereinbaren die Parteien wie folgt:

Der Auftragnehmer erbringt Datenverarbeitungen im Rahmen der technischen und administrativen Leistungen für die Bereitstellung und den Betrieb eines Security Operation Center (SOC). Das SOC bildet die zentrale Organisationseinheit für die Detektion und Reaktion auf Sicherheitsvorfälle in den angeschlossenen Quellen. Zur Optimierung und Automatisierung der Sicherheitsprozesse setzt der Auftragnehmer ein SOAR-Tool (Security Orchestration, Automation, and Response) ein, das eine effiziente Koordination zwischen den verschiedenen Sicherheitssystemen ermöglicht, automatisierte Reaktionen auf Vorfälle ausführt und die Dokumentation von Maßnahmen unterstützt.

Zur Anreicherung und Kontextualisierung sicherheitsrelevanter Ereignisse nutzt der Auftragnehmer zudem Threat Intelligence Plattformen. Diese ermöglichen die Korrelation und Analyse von Bedrohungsinformationen aus den verschiedenen Quellen und unterstützt damit die Entscheidungsfindung im SOC sowie die Priorisierung von Maßnahmen.

Bei den angeschlossenen Quellen handelt es sich insbesondere, aber nicht abschließend, um ein SIEM (einschließlich UEBA), ein EDR/XDR (einschließlich Anti-Virus), eine NGFW oder ein IDS/IPS. Die an das SOC angeschlossenen Quellen sind abhängig von der Beauftragung des Auftraggebers.

Der Auftragnehmer erbringt des Weiteren Datenverarbeitungen im Auftrag gemäß der Leistungsbeschreibung zu folgenden Zwecken:

- Security Monitoring (Level 1 & 2)
- Alerting und Eventmanagement
- Threat Hunting
- Security Incident Response Support
- Quellen-Überwachung

1.3 Art der Auftragsdaten:

Die Auftragsverarbeitung betrifft folgende Arten personenbezogener Daten[1]:

Die Arten der im Rahmen der Serviceerbringung verarbeiteten personenbezogenen Daten sind im Vorfeld nicht exakt zu bestimmen. Die Datenarten hängen von der Art der an das SOC angeschlossenen Quellen, den Anfragen des Auftraggebers, und von den durch den Auftraggeber selbst im Einzelfall zur Verfügung gestellten personenbezogenen Daten ab.

Im Rahmen der Leistungserbringung kommt es in jedem Fall – jedoch nicht abschließend – zur Verarbeitung der folgenden Datenkategorien:

- Stamm- und Kontaktdaten (z. B. Name, E-Mail-Adresse)
- Login-Daten (z. B. Username, Passwort)
- IT-Nutzungsdaten (z. B. Protokolldaten, IP-Adresse, User-ID, Geräte-ID)
- An- und Abmeldedaten (erfolgreiche oder fehlgeschlagene Anmeldung)
- Rechteänderung (Auditlogs) und Aufruf von Tools
- Log-Daten über Zugriffe auf Dateien und Ressourcen auf Ebene der Clients, VDIs und Server (z. B. Informationen zu Abweichungen/Blockaden/fehlgeschlagenen Zugriffen, Zeitpunkt des Zugriffes)
- Verbindungsdaten (bspw. Proxylogs, VPN-Logs, Firewall-logs)

Besondere Kategorien personenbezogener Daten

☐ Die Auftragsverarbeitung betrifft keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO.

☒ Die Auftragsverarbeitung betrifft die folgenden besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO:

Es kann im Vorfeld nicht ausgeschlossen werden, dass besondere Kategorien personenbezogener Daten im Rahmen eines Incident Response zufällig durch den Auftragnehmer verarbeitet werden, sofern sich auf einem isolierten Host/Client besondere Kategorien personenbezogener Daten befinden.

1.4 Kategorien der von der Auftragsverarbeitung betroffenen Personen

Die Auftragsdaten betreffen die personenbezogenen Daten folgender Kategorien betroffener Personen:

Die Kategorien von betroffenen Personen hängen von den an das SOC angeschlossenen Quellen des Auftraggebers ab. Es ist daher möglich, dass z. B. personenbezogene Daten von Mitarbeitenden des Auftraggebers oder Mitarbeitenden der Lieferanten/Kunden des Auftraggebers verarbeitet werden können.

[1] Zu den besonderen Kategorien personenbezogener Daten gehören: Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische Daten, biometrische Daten, Gesundheitsdaten und Daten mit Bezug zum Sexualleben oder der sexuellen Orientierung.

2. Bezeichnung der Unter-Auftragnehmer

☐ Im Rahmen der Auftragsverarbeitung werden keine Unter-Auftragnehmer eingesetzt.

☒ Gemäß Ziffer 8 der Rahmenvereinbarung über die Auftragsverarbeitung werden im Rahmen der Auftragsverarbeitung die nachfolgenden aufgelisteten Unter-Auftragnehmer eingesetzt.

Folgende Unter-Auftragnehmer verarbeiten die Auftragsdaten im Auftrag des Auftragnehmers für Teilleistungen der Auftragsverarbeitung:

Unter-Auftragnehmer	Anschrift (Stadt/Land)	Bezeichnung der Auftragsleistungen
Cyfidelity Security Services GmbH	Bechterdisser Straße. 10 33719 Bielefeld	▪ Sicherheitsdienstleistungen zur Erkennung, Analyse und Abwehr von IT-Sicherheitsbedrohungen – beispielsweise im Bereich Digital Forensics und Incident Response
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay Dublin 2 Ireland	▪ Bereitstellung und Betrieb des Google SOAR sowie weiterer SecOps Services auf der Google Cloud Platform ▪ Herstellersupport und Troubleshooting
NoVirusThanks Company Srl	VIA CANNAVA 86 43043 Borgo Val Di Taro Perugia Italien	▪ Bereitstellung und Betrieb der Threat Intelligence Plattform APIVoid

3. Liste der gestatteten Auftragsverarbeitungen in Drittländern

☐Es finden keine Datenverarbeitungen im Rahmen der Auftragsverarbeitung in Drittländern statt.

☒Nach Maßgabe von Ziffer 2 der Vereinbarung erteilt der Auftraggeber seine Zustimmung zur Durchführung von Teilleistungen der Auftragsverarbeitung durch den Auftragnehmer und/oder Unter-Auftragnehmer in den nachfolgend bezeichneten Drittländern:

Bezeichnung Auftragnehmer oder Unter-Auftragnehmer	Bezeichnung der Auftragsleistungen, die in Drittländern erbracht werden	Bezeichnung Drittland
Google Cloud EMEA Limited	▪ Bereitstellung und Betrieb des Google SOAR sowie weiterer SecOps Services auf der Google Cloud Platform ▪ Herstellersupport und Troubleshooting	▪ **Bereitstellung und Betrieb des Google SOAR sowie weiterer SecOps Services auf der Google Cloud Platform** Für die Bereitstellung und den Betrieb des Google SOAR sowie weiterer SecOps-Services auf der Google Cloud Platform wurde die Data Center Location EU gewählt. Im Rahmen des Betriebs dieser Services kann es durch den Einsatz von weiteren Unter-Auftragnehmern zu einer Datenübermittlungen in Drittländer kommen. Die aktuelle Liste der eingesetzten Unter-Auftragnehmer der Google Cloud Platform ist einsehbar unter Google Cloud Platform Subprocessors | Google Cloud. Die Liste der speziell für die SecOps-Services eingesetzten Unter-Auftragnehmer ist einsehbar unter SecOps Services Subprocessors | Google Cloud. ▪ **Herstellersupport und Troubleshooting** Der Herstellersupport sowie das Troubleshooting der Google Cloud Platform können – abhängig von Art und Umfang der Supportleistungen sowie den jeweiligen Supportzeiten – durch Googles Unter-Auftragnehmer in verschiedenen Drittländern erfolgen.

		Im Rahmen dieser Supportleistungen erhalten die von Google eingesetzten Unter-Auftragnehmer keinen direkten Zugriff auf gespeicherte Kundendaten. Weitere Informationen zu den eingesetzten Unter-Auftragnehmer sind ebenfalls unter folgendem Link einsehbar: Google Cloud Platform Subprocessors | Google Cloud Datenübermittlungen in Drittländer erfolgen unter Einhaltung der geltenden datenschutzrechtlichen Vorgaben und werden durch geeignete Garantien gemäß Art. 44 ff. DSGVO abgesichert. Umfassende Informationen zum Datenschutz in der Google Cloud sind einsehbar unter Datenschutz-Center | Google Cloud Der Geltungsbereich der Google Compliance Programme für die SecOps-Services ist einsehbar unter SecOps Services in Scope by Compliance Program | Google Cloud
NoVirusThanks Company Srl	▪ Betrieb und Bereitstellung der Threat Intelligence Plattform APIVoid	Im Rahmen der Bereitstellung und des Betriebs der Threat Intelligence Plattform APIVoid erfolgen Übermittlungen personenbezogener Daten in die USA. Die Datenübermittlung erfolgt im Rahmen der geltenden datenschutzrechtlichen Vorgaben, insbesondere unter Berücksichtigung geeigneter Garantien gemäß Art. 44 ff. DSGVO.

4. Ergänzende Vereinbarungen zu Service-bezogenen technischen und organisatorischen Maßnahmen

☒ Im Rahmen der Erbringung der Service-Leistungen wird der Auftragnehmer die in Anlage 2 der Rahmenvereinbarung definierten technischen und organisatorischen Maßnahmen treffen, um die Sicherheit der Auftragsverarbeitung gemäß Art. 32 DSGVO zu gewährleisten.

☐ Ergänzend zu den in Anlage 2 der Rahmenvereinbarung definierten technischen und organisatorischen Maßnahmen wird der Auftragnehmer im Rahmen der Erbringung der Service-Leistungen die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen treffen, um die Sicherheit der Auftragsverarbeitung gemäß Art. 32 DSGVO zu gewährleisten.

Beschreibung der Service-bezogenen technischen und organisatorischen Maßnahmen:

☐ Anstelle der in Anlage 2 der Rahmenvereinbarung definierten technischen und organisatorischen Maßnahmen wird der Auftragnehmer im Rahmen der Erbringung der Service-Leistungen die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen treffen, um die Sicherheit der Auftragsverarbeitung gemäß Art. 32 DSGVO zu gewährleisten.

Beschreibung der Service-bezogenen technischen und organisatorischen Maßnahmen: