# Leistungsbeschreibung
# Magenta Security Shield Smart

Stand: 10.03.2025

## 1 Einleitung

Die Telekom Deutschland GmbH (im Folgenden Telekom genannt) stellt mit dem standardisierten Sicherheitsservice Magenta Security Shield Smart powered by Cynet Security Ltd. als Unterauftragnehmer der Telekom, (powered by Cynet) einen Managed Security Service auf der Grundlage von Software-as-a-Service (im Folgenden „SaaS“ genannt) zur Verfügung, der Angriffe auf die IT-Umgebung des Kunden erkennen, abwehren und die Einleitung von Gegenmaßnahmen unterstützen soll. Ein Endpunkt-Scanner erfasst und liefert Meta-Daten für die Überwachung an ein Backend. Zudem können verdächtige Aktivitäten auf dem Endpunkt erkannt sowie Gegenmaßnahmen direkt auf den IT-Endgeräten des Kunden (z. B. Arbeitsplätze, Server), im Folgenden Endpunkte genannt, ausgeführt werden. Der Service verwendet standardisierte Korrelationsregeln (Policies) und Bedrohungsszenarien (Use Cases). Die Überwachung erfolgt auf Betriebssystemebene. Magenta Security Smart Shield beinhaltet:

- eine in der Telekom Cloud betriebene Sicherheitslösung, basierend auf dem Einsatz von Endpunkt-Scannern, die auf den Endpunkten des Kunden installiert werden
- einen Security Operations Center (SOC) Service der Telekom
- sowie technischen Support der Telekom.

Voraussetzung zur optimalen Nutzung der Leistung ist die lückenlose Nutzung aller Endgeräte beim Kunden, die aktiv mit der Leistung von Magenta Security Shield Smart überwacht werden. Der Kunde muss mindestens 25 Endpunkte abnehmen (Mindestabnahme). Für die Nutzung von Magenta Security Shield Smart gelten auf Kundenseite u. a. die nachfolgend aufgeführten technischen Voraussetzungen:

- Internetzugang
- aktueller Internet-Browser

Der für den Zugang zur Cloud-Plattform erforderliche Anschluss und die Verbindungen sowie das erforderliche Kommunikations-Equipment sind nicht Gegenstand dieses Vertrages und müssen auf Kundenseite bereitgestellt werden.

## 2 Funktionen

Die Unternehmen begegnen heutzutage sich permanent verändernden Sicherheitsbedrohungen über multiple Angriffsvektoren hinweg. Präventive Maßnahmen allein bieten davor keinen ausreichenden Schutz mehr. Davon ausgehend, dass Cyber Angriffe nicht vollständig verhindert werden können, rückt die Erkennung von Bedrohungen und Sicherheitsvorfällen in den Fokus. Diese Erkennung erfolgt mithilfe eingesetzter Technologie und dem Telekom SOC (Security Operation Center). Dort werden Zusammenhänge sichtbar gemacht und von Sicherheitsexperten situationsbedingte Handlungsalternativen erstellt und dem Kunden übermittelt. Der Service kombiniert automatisierte und manuelle Analysen von Alarmen aus den IT-Systemen des Kunden. Zusätzlich werden aktuelle Threat Intelligence Informationen genutzt, um die Qualität der Analysen zu steigern.

### 2.1 Technologie

Magenta Security Shield Smart besteht aus einem zentralen SaaS Backend und Scannern, die auf den zu überwachenden Endpunkten durch den Kunden installiert werden und über das Internet mit dem Backend kommunizieren. Das Backend bietet folgende Funktionalitäten.

#### 2.1.1 Server und Kunden-Managementkonsole

Der Server ist verantwortlich für die Frontend-Services jedes virtuellen Mandanten. Jeder Mandanten-Service wird über einen Token den Endpunkten zugewiesen und verfügt über eine eigene Datenbank. Dieser Server fungiert als Frontend-Service für den betreffenden Mandanten und ist verantwortlich für die Verarbeitung der Eingangsdaten der mit einem Scanner geschützten Assets (Hosts, Dateien, Nutzer, Netzwerk). Über den Server kann der Kunde auf die

Managementkonsole im Lesemodus zugreifen. Die Managementkonsole bietet eine korrelierte Übersicht der Assets in der Kundenumgebung.

#### 2.1.2 Virtual Private Cloud (VPC)

Die VPC befindet sich in der Cloud des Unterauftragnehmers Cynet Security Ltd. Dieses System übernimmt verschiedene Funktionen.

- Cyber-Bedrohungsanalyse in Form von Indicators of Compromise (IoCs), hierzu zählen maliziöse IP Adressen in Verbindung mit Angriffen, malware-verbreitende Seiten und Command & Control Server.
- Updates einschließlich aktualisierte Abwehr- und Erkennungskapazitäten zur Einleitung von Gegenmaßnahmen auf neue Bedrohungen.
- Support bei der forensischen Untersuchung und Reaktion auf erzeugte Warnmeldungen (Alarme).
- Weiterleitung von ausgewählten Dateien in eine Sandbox.
- Weiterleitung von mobilen Telefonnummern zur Einrichtung der Multifaktor-Authentifizierung per SMS.

Eine Weiterleitung von personenbezogenen und/oder -beziehbaren Daten im Sinne des Datenschutzes von den Mandanten zur Cynet VPC mit Ausnahme der Mobilfunknummern für die Multifaktor-Authentifizierung erfolgt nicht. Daten werden vor der Weitergabe anonymisiert oder gänzlich von der Weiterleitung ausgeschlossen. Diese anonymisierten Daten dienen forensischen Zwecken, um Gegenmaßnahmen zu optimieren. Die Datenübertragung erfolgt über das Internet stets in verschlüsselter Form.

#### 2.1.3 Zugriffsmöglichkeiten bei Gegenmaßnahmen

Zur Erbringung der SOC-Leistungen können durch Magenta Security Shield Smart umfangreiche manuelle Aktionen als Reaktion auf Sicherheitsvorfälle auf den Endpunkten ausgeführt werden. Diese manuellen Aktionen werden dem Kunden vorab durch die Telekom angezeigt und nur bei vorliegender Einwilligung des Kunden durchgeführt, es sei denn, die autorisierten Ansprechpartner des Kunden sind nicht erreichbar oder es besteht Gefahr in Verzug. Durch das Ausführen von Kommandos oder Skripten mit administrativen Privilegien kann prinzipiell auf alle Daten der überwachten Endpunkte zugegriffen und weitreichende Aktionen auf dem Endpunkt ausgeführt werden. Diese weitreichenden Möglichkeiten stehen den Mitarbeitern der Telekom sowie denen des Unterauftragnehmers, welcher den Betrieb des Backend durchführt, zur Verfügung.

### 2.2 Features

Mit Magenta Security Shield Smart werden kontinuierlich Daten in der Kundenumgebung erfasst und analysiert. Dies sind Daten zur Ausführung von Anwendungen und Prozessen, zum Netzverkehrsverhalten der Endpunkte, zur Benutzerkontenaktivität und zum Dateizugriff. Diese Daten schaffen eine Transparenz über die überwachte Kundenumgebung und ermöglichen somit eine proaktive Erkennung und die Überwachung von möglichen Angriffsflächen. Magenta Security Shield Smart übermittelt diese Daten der Endpunkte an die Plattform in der Telekom Cloud und führt sie dort zusammen, um den Kontext jedes Einzelereignisses herzustellen. So wird eine Angriffserkennung und -vermeidung mit hoher Genauigkeit erzielt und die Alarmanalyse optimiert. Magenta Security Shield Smart beinhaltet die folgenden technischen Funktionen.

#### 2.2.1 Überwachung (Monitoring & Control)

Magenta Security Shield Smart automatisiert die Erfassung und Korrelation von ausgeführten Dateien, Prozessen, Nutzer-Aktivitäten, Datenzugriffen und Netzverkehren mit dem Ergebnis, dass alle Überwachungsabläufe beschleunigt und vereinfacht werden. Magenta Security Shield Smart führt die Bewertung von Sicherheitslücken auf der Grundlage der von Endpunkt-Scannern gesammelten Daten durch, so dass weder ein aktiver, serverseitiger Scan noch zusätzliche e Softwarekomponenten erforderlich sind. Es können Berichte zu Sicherheitslücken bei Anwendungen und Systemen, die diese für bekannte Angreifer anfällig machen, erstellt werden. Der Service speichert sicherheitsbezogene Aktivitätsprotokolle, beispielsweise erfolgreiche und fehlgeschlagene Anmeldungen, Softwaredownloads,

Passwortänderungen sowie die weiteren definierten Aktivitäten. Jeder Scanner sammelt die Aktivitätsprotokolle des jeweiligen Endpunkts und übermittelt diese zur Weiterverarbeitung verschlüsselt an die Plattform im Telekom Rechenzentrum. Der Service bietet eine granulare Übersicht über den physischen und virtuellen IT-Bestand aller geschützten Endpunkte. Die Bestandsdaten können über eine Managementkonsole dargestellt und für die weitere Verarbeitung durch den Kunden exportiert werden.

### 2.2.2 Angriffserkennung und -vermeidung (Attack Detection & Prevention)

Magenta Security Shield Smart nutzt die Sichtbarkeit aller Endpunkt-, Netz- und Nutzeraktivitäten in der durch Endpunkt-Scanner geschützten IT-Umgebung des Kunden zur Erkennung und Vermeidung von Angriffsvektoren. So werden nativ die Kernfunktionen EDR inkl. NGAV, UBA, Netzwerkanalyse und Täuschung (Deception) implementiert und im Ergebnis eine Erkennung von Angriffen mit hoher Genauigkeit ermöglicht. Next Generation Anti-Virus (NGAV) umfasst mehrfache Angriffsvermeidungstechnologien, um eine größtmögliche Abdeckung der Punkte zu erreichen, an denen Standard- und Zero-Day-Angriffe beendet werden können.

- Bekannte Schadsoftware: Identifikation und Vermeidung der Ausführung von Schadsoftware mit bekannten Signaturen.
- Fuzzy Hashing: Identifikation von Dateien mit großer Ähnlichkeit zu bekannten Malware-Hashes.
- Speicherzugriffskontrolle: Gewährleistung, dass Prozesse auf ausschließlich für sie zulässige Speicherbereiche zugreifen können.
- Auf Algorithmen basierende statische Analyse: Dateianalyse vor der Ausführung zur Erkennung maliziöser Attribute.
- Verhaltensanalyse: Prozessüberwachung zur Laufzeit und Beendigung bei Erkennung von bösartigem Verhalten.
- Anti-Ransomware: Bekannte Ransomware-Angriffe werden erkannt und gestoppt.

Die Endpoint Detection & Response (EDR) Funktion überwacht die Endpunkte kontinuierlich, so dass die Endpunkt-Scanner bösartige Aktivitäten erkennen und eine Alarmierung, sowie ggf. automatische Gegenmaßnahmen, ausführen können. EDR stellt den Kontext für eindeutige Warnmeldungen bereit:

- Korrelation: EDR erzeugt Sichtbarkeit von Programmausführungen, Netzwerkdatenströmen und Nutzeraktivitäten.
- Validierung: Auf der Grundlage der Korrelation all dieser Aktivitätssignale kann verdächtiges Verhalten validiert werden, sogar schon bevor Alarme erzeugt werden.
- Alarm: Nach Erzeugung eines Alarms wird der gesamte erforderliche Kontext zur Verfügung gestellt, um die Ereignisse schnell und effizient zu sortieren, zu priorisieren und weitere Schritte planen zu können.

Gegenmaßnahmen können auf dem Endpunkt entweder automatisch, anhand von vordefinierten Aktionen bei Erzeugung eines Alarms ausgeführt werden, oder bei Bedarf und nach Rücksprache mit dem Kunden manuell durch das Telekom SOC. Das Monitoring des Nutzerverhaltens (User Behavior Analytics, UBA) bietet die Möglichkeit, Nutzeraktivitäten kontinuierlich zu überwachen. Alarme werden erzeugt, sobald untypische Signale erkannt werden, die auf kompromittierte Nutzerkonten hindeuten. Die Netzwerkanalyse überwacht kontinuierlich den Netzverkehr am Endpunkt, um verdächtige, oder gar bösartige Aktivitäten zu erkennen und zu blockieren. Der durch die Netzwerkanalyse gewährleistete Schutz ist geeignet, fortgeschrittene Angriffsszenarien an den geschützten Endpunkten zu detektieren. Zur Anwendung kommen insoweit Netzsichtbarkeit, Verhaltensanalyse, deterministische Module und Angriffserkennung. Hierzu zählen Auskundschaftung (Reconnaissance) durch einen Angreifer, Diebstahl von Anmeldedaten, Lateral Movement-Aktivitäten, Verbindungen zu kritischen externen Systemen oder Daten-Exfiltration.

### 2.2.3 Täuschungstechnologien

Durch den Einsatz von Täuschungstechnologien können zusätzlich Angriffe erkannt werden. Köderdateien (Decoys) können in den Dateisystemen der Endpunkte platziert werden, welche bei Verwendung Alarme auslösen.

### 2.2.4 Black-/Whitelisting

Magenta Security Shield Smart verfügt über eine Black-/Whitelisting-Funktion, mithilfe derer bekannte Domänen oder IP-Adressen geblockt oder explizit zugelassen werden können. Somit kann der Zugriff auf bekannte maliziöse, aber auch unerwünschte Ziele generell für die überwachten Endpunkte gesperrt oder auch zugelassen werden. Die Telekom behält sich das Recht vor, Blacklists bei offensichtlichen, wiederkehrenden Angriffen zu erweitern und somit den Zugriff auf verifizierte maliziöse Ziele für die überwachten Endpunkte zu blockieren. Dies kann eingeschränkt erfolgen, so dass für spezifische Nutzergruppen die Sperre nicht wirksam wird.

### 2.2.5 Risk Scoring

Das Risk Scoring ist eine proaktive Maßnahme zur Vorbeugung (Prevention) und zur Verbesserung der Resilienz der IT-Umgebung gegenüber Angriffen. Der Score wird durch viele einzelne Indikatoren über alle überwachten Assets (Hosts, Dateien, Nutzer, Netzwerk) gebildet. Somit kann der Kunde den Fokus der eigenen Analyse auf die als besonders gefährdet eingestuften Assets richten, auch wenn keine Alarme oder erfolgreichen Angriffe vorliegen. Durch einen Gesamt-Risk Score wird die Sicherheitslage des Unternehmens stets aktuell abgebildet.

### 2.2.6 Automatisierte Gegenmaßnahmen (Auto-Remediation)

Durch Magenta Security Shield Smart können Gegenmaßnahmen bei Sicherheitsvorfällen, wie infizierten Endpunkte oder Zugriff auf bösartige Internetdienste, eingeleitet werden. Magenta Security Shield Smart verfügt über eine umfangreiche Anzahl von Regeln (Policies), welche Alarme erzeugen, sobald die hinterlegten Indikatoren erkannt werden. Zu vielen dieser Alarme sind Gegenmaßnahmen definiert, die an den Endpunkten automatisch ausgeführt werden können, wenn die „Auto-Remediation“-Funktionen aktiviert sind. Somit kann beispielsweise ein Ransomware-Prozess automatisch beendet werden, noch bevor dieser einen größeren Schaden anrichtet, oder der Zugriff auf bösartige Web-Ressourcen unterdrückt werden. Es ist empfehlenswert, automatische Gegenmaßnahmen für möglichst viele Endpunkte zu aktivieren, um einen möglichst maximalen Schutz in Fast-Echtzeit zu erreichen. Sollten diese Funktionen für kritische Systeme nicht geeignet sein, können solche Systeme ausgenommen werden. Dies ermöglicht eine spezifische Anwendung der Funktion abgestimmt auf das Sicherheitsbedürfnis des Kunden. Der Kunde benennt die auszuschließenden Systeme eigenverantwortlich im Onboarding-Prozess oder meldet diese beim technischen Support nach. Während des Onboarding-Prozesses (siehe Abschnitt 3.1.2) wird die Einwilligung des Kunden zur Aktivierung der automatisierten Gegenmaßnahmen schriftlich oder mit qualifizierter elektronischer Signatureingeholt, nachdem das System einen ausreichenden Stabilitätsgrad erreicht hat und Fehlalarme minimiert wurden. Der Kunde ist somit für die durch diese Funktion automatisch ausgelösten Auswirkungen selbst verantwortlich.

### 2.2.7 Managementkonsole

Magenta Security Shield Smart verfügt über eine Managementkonsole. Sie gibt einen Überblick über die Gesamtsicherheitssituation der überwachten Endpunkte des Kunden. Aktuelle Bedrohungen werden optisch in einem Radar dargestellt. Die aktuelle Alarmverteilung über Zeit und Schweregrad sowie die Anzahl der geschützten Hosts werden angezeigt. Zwei autorisierte Ansprechpartner des Kunden erhalten lesenden Zugriff auf die Magenta Security Shield Smart Managementkonsole. Sie können Alarmdaten sowie die gesammelten und korrelierten Asset-Daten (Host-, Prozess-, Nutzer- und Netzwerkaktivitäten) der Kundenumgebung einsehen und das Risk Scoring nutzen, um potenzielle Gefährdungen eigenständig zu verringern.

### 2.2.8 Berichte

Mit Magenta Security Shield Smart können die autorisierten Ansprechpartner eigenständig Berichte erzeugen und exportieren.

- Alarmbericht: Eine Auswertung aller aufgekommenen Alarme, in einem selbst definierten Zeitraum. Darunter fallen: Alarme nach Typ, Status, Datum, Top Alarme und Alarm Data.
- Top-Risikobericht: Eine Auswertung aller Risiken in einem selbst definierten Zeitraum: Konkret werden die Top 10 Risiko-Dateien angezeigt.

- Schwachstellenbewertungsbericht:
  - Auswertung Missing KBs On Host (Fehlende Windows Updates)
  - Auswertung Agent Validation
  - Auswertung Application Patch Validations
  - Auswertung Unauthorized Applications
- Inventarbericht: Eine Auswertung aller Endgeräte mit Namen, OS, CPU (%), Arbeitsspeicher, Arbeitsspeicher (%), System Partitionsgröße und freiem Speicherplatz.

Die Berichte können in der Managementkonsole eingesehen und heruntergeladen werden.

## 2.3 Service-Module des Basispaketes

Neben den technischen Funktionen enthält Magenta Security Shield Smart die hier aufgelisteten Serviceanteile

### 2.3.1 Threat Intelligence

Magenta Security Shield Smart erhält regelmäßig aktualisierte Sicherheitsinformationen (Indicators of Compromise) aus zahlreichen und verschiedenen Quellen, die für die Bereitstellung einer effektiven Cyber-Sicherheitslösung notwendig sind. Diese Informationen ermöglichen es, schnell und effektiv auf Veränderungen der Sicherheitslage zu reagieren und somit hochwertige Alarme zu erhalten.

### 2.3.2 Security Operations Center Services

Sicherheitsvorfälle zu erkennen und darauf zu reagieren ist eine zentrale Leistung des Magenta Security Shield Smart Service der Telekom. Sie besteht aus der permanenten Überwachung der im System eingehenden Alarme der Schweregrade „Kritisch“ und „Hoch“. Als Ergebnis der dann folgenden Alarmanalyse werden überprüfte Sicherheitsvorfälle an den Kunden weitergeleitet. Dies erfolgt über eine definierte Schnittstelle per E-Mail an ein zentrales E-Mail-Postfach des Kunden. Im Fall von besonders kritischen Sicherheitsvorfällen kann der Kunde durch das Telekom SOC per Telefon kontaktiert werden. Voraussetzung ist insofern, dass ein autorisierter Ansprechpartner mit Mobilfunknummer (Ziffer 3.1.4) hinterlegt ist, der im Rahmen des Onboardings vom Kunden mitgeteilt werden kann. Keine Benachrichtigung erfolgt bei Alarmen, deren Prüfung keinen Sicherheitsvorfall (z. B. Fehlalarme) ergeben. Arbeiten des Kunden in seiner IT-Umgebung oder an seinen Endpunkten sind zur Vermeidung von unbeabsichtigten Sicherheitsvorfällen von den Ansprechpartnern des Kunden der Telekom rechtzeitig vorher mitzuteilen.

#### 2.3.2.1 Definition Sicherheitsvorfall (Event)

Ein Sicherheitsvorfall ist eine Korrelation von einem oder mehreren überprüften Alarmen bezogen auf die in den Detektionsszenarien definierten Regeln. Jedem Sicherheitsvorfall ist ein Schweregrad zugeordnet, dieser ist im Detektionsszenario festgelegt. Es werden folgende Schweregrade bei Sicherheitsvorfällen unterschieden:

- Kritisch: Sicherheitsvorfälle, die sofortige Reaktion erfordern, um schwerwiegende Auswirkungen zu lindern (z. B. im Falle einer erkannten Ransomware in der Kundenumgebung).
- Hoch: Sicherheitsvorfälle, die die Aufmerksamkeit des Kunden erfordern (z. B. bei Erkennung einer verdächtigen Aktivität, die weitergehende Untersuchung benötigt).

Der Schweregrad eines Sicherheitsvorfalls definiert die Priorisierung der Bearbeitung der Alarme gemäß den unten definierten Reaktionszeiten des Telekom SOC.

#### 2.3.2.2 Vorgehensweise des Telekom SOC

Die in Magenta Security Shield Smart generierten Alarme mit den Schweregraden „High“ und „Critical“ werden der Analyse unterworfen. Diese Alarme werden dann im Rahmen der vereinbarten SLA-Zeit nach standardisierten Verfahren bearbeitet. Sollten während der Analyse zusätzliche Informationen vom Kunden benötigt werden, oder nach Durchlauf aller Analyseschritte die Benachrichtigung über einen Sicherheitsvorfall notwendig sein, wird der Kunde per E-Mail oder,

falls aus Sicht der Telekom erforderlich und sofern möglich, per Telefon informiert. Alarme eines geringeren Schweregrades („Medium“, „Low“ und „Informative“) werden lediglich als zusätzliche Informationsquelle bei der SOC-Analyse schwerwiegenderer Alarme hinzugezogen.

#### 2.3.2.3Durchführung von manuellen Gegenmaßnahmen

Sollten im Rahmen der Alarmbearbeitung Gegenmaßnahmen notwendig sein, die ggf. über bereits erfolgte automatische Gegenmaßnahmen hinausgehen, wird das Telekom SOC den Kunden über weitere, geeignete Maßnahmen informieren. Nach vorliegender Einwilligung durch den Kunden können mithilfe von Magenta Security Shield Smart die abgestimmten Gegenmaßnahmen auf den Endpunkten in der Kundenumgebung durchgeführt werden. Der Kunde ist somit für die durch diese Maßnahmen ausgelösten Auswirkungen selbst verantwortlich. Falls folgende Voraussetzungen vorliegen, stimmt der Kunde zu, dass das Telekom SOC berechtigt ist, auch ohne vorliegende ausdrückliche Einwilligung des Kunden manuelle Gegenmaßnahmen durchzuführen:

- Der Kunde ist innerhalb eines angemessenen Zeitraums nicht erreichbar und/oder
- Die Schwere des Vorfalls lässt nach Einschätzung des Telekom SOC keinen weiteren Verzug zu.

Der Kunde wird im Nachgang über die erfolgten Maßnahmen informiert. Durch das Ausführen von Kommandos oder Skripten mit administrativen Privilegien im Rahmen der Alarmbearbeitung kann prinzipiell auf alle Daten der überwachten Endpunkte zugegriffen und weitreichende Aktionen auf dem Endpunkt ausgeführt werden. Diese weitreichenden Möglichkeiten stehen den Mitarbeitern der Telekom sowie denen des Unterauftragnehmers, welcher den Betrieb des Backend durchführt, zur Verfügung.

## 2.4 Endpunkt-Scanner und Softwareupdates

Für die Nutzung der verschiedenen Funktionen ist die Installation einer Endpunkt-Scanner auf den jeweiligen Endgeräten notwendig. Die Leistungen von Magenta Security Shield Smart werden für unterstützte Betriebssysteme bereitgestellt. Eine Auflistung der aktuell unterstützten Betriebssysteme ist der nachfolgenden Liste der aktuell unterstützten Betriebssysteme zu entnehmen. Während des Onboardings berät das Telekom Support Team den Kunden zu verschiedenen technischen Möglichkeiten des Rollouts und der Installation der Endpunkt-Scanner. Die Installation der Endpunkt-Scanner auf den zu überwachenden Endpunkten obliegt dem Kunden. In unterschiedlichen Abständen stehen dem Kunden Softwareupdates für die Endpunkt-Scanners zur Verfügung. Softwareupdates können automatisch installiert werden. Der Download und die Installation des Updates der Endpunkt-Scanners ist zwingende Voraussetzung für die Sicherstellung, dass der Kunde die aktuelle Fassung der Leistungen nutzen und von den neuesten Funktionalitäten Gebrauch machen kann. Die Telekom weist darauf hin, dass die Funktionalität nicht oder nur eingeschränkt nutzbar ist, wenn die Installation der Updates unterbleibt. Die Telekom kann im Fall der Nichtdurchführung von Updates die Funktionalitäten der Lösung nicht gewährleisten und ist für sich daraus ergebende Leistungseinschränkungen von Magenta Security Shield Smart nicht verantwortlich.

### 2.4.1 Liste der aktuell unterstützten Betriebssysteme

Die Endpunkt-Scanner können über die Managementkonsole bezogen werden. Sie stehen für die Betriebssysteme Windows, MacOS und Linux bereit. Folgende Versionen werden aktuell unterstützt.

- Windows (32/64 bit); Linux (32/64 bit); Mac (64 bit); Windows 7 SP2 und höher (zusätzlich werden die Patches KB4490628 und KB4474419 benötigt); Red Hat 6.9 und höher; OS X Mavericks; Windows 8 und 8.1; Fedora 21 und höher; OS X Yosemite; Windows 10; Ubuntu 16.04 und höher; OS X El Capitan; Windows 11; CentOS 6.9 und höher; MacOS Sierra; Windows Server 2008 / 2008 R2; SUSE 12.0 und höher; MacOS High Sierra; Windows Server 2012 / 2012 R2; Debian 9.0 und höher; MacOS Mojave; Windows Server 2016; Oracle Enterprise Linux 7.6 und höher; MacOS Catalina; Windows Server 2019; Amazon Linux; MacOS Big Sur; Windows Server 2022; Amazon Linux 2

Sysdig wird von Cynet auf Oracle Enterprise Linux 7.6 und höher, Amazon Linux und Amazon Linux 2, nicht unterstützt. Unterstütze Systeme für das CISO Kit: iOS 10.0 und höher iPadOS 10.0 und höher watchOS 4.3 und höher.

Die Telekom aktualisiert die Software von Magenta Security Shield Smart ständig, um sie an neue oder aktualisierte Versionen der Betriebssysteme anzupassen. Ältere Betriebssystemversionen werden möglichst lange unterstützt. Dennoch ist es aus technischen Gründen nicht möglich, die Lauffähigkeit auf veralteten Betriebssystemversionen unbegrenzt zu unterstützen. Die Telekom behält sich daher vor, die Unterstützung für veraltete Betriebssystemversionen einzustellen; insbesondere, wenn der Service (z. B. Sicherheitsupdates) für das betroffene Betriebssystem vom Hersteller nicht mehr erbracht wird. Aus diesem Grund sind ältere Betriebssysteme nicht mit aufgeführt, obwohl sie vom Hersteller derzeit noch unterstützt werden. Es liegt in der Verantwortung des Kunden, die Lauffähigkeit auf spezifischen Softwarekombinationen vor einem geplanten Produktiveinsatz zu überprüfen. Sofern der Kunde ein anderes, als die in der vorstehenden Tabelle aufgeführten Betriebssysteme einsetzt, weist Telekom ausdrücklich darauf hin, dass die Funktionalitäten von Magenta Security Shield Smart nicht oder nur eingeschränkt nutzbar sein können und Sicherheitslücken auftreten können. Auch wenn die Lösung mit älteren Betriebssystemen eingangs funktioniert, kann Telekom den Schutz für nicht in der Tabelle aufgeführte Betriebssysteme nicht gewährleisten und ist für sich daraus ergebende Leistungseinschränkungen von Magenta Security Shield Smart nicht verantwortlich.

## 3 Leistungen der Telekom

Magenta Security Shield Smart beinhaltet die vom Unterauftragnehmer in der Telekom Cloud betriebene Sicherheitslösung und Endpunkt-Scanner, die im Netzwerk des Kunden installiert werden. Zudem bietet Magenta Security Shield Smart einen Telekom Security Operations Center Service (SOC Service) und technischen Support.

### 3.1 Bereitstellung

Die Leistungen von Magenta Security Smart Shield gelten nach Durchführung des Kickoff-Workshops als bereitgestellt. Zu diesem Zeitpunkt ist der Mandant eingerichtet und der Kunde kann die Endpunkt-Scanner zur Überwachung der Endpunkte in der eigenen IT-Umgebung ausrollen.

#### 3.1.1 Zugang

Die Leistungen von Magenta Security Smart Shield gelten nach Durchführung des Kickoff-Workshops als bereitgestellt. Zu diesem Zeitpunkt ist der Mandant eingerichtet und der Kunde kann die Endpunkt-Scanner zur Überwachung der Endpunkte in der eigenen IT-Umgebung ausrollen.

#### 3.1.2 Einrichtung von Magenta Security Shield Smart (Onboarding)

Vor der Betriebsaufnahme von Magenta Security Shield Smart ist ein in mehreren Prozessschritten aufgeteiltes Onboarding des Kunden erforderlich; während dieser Phase wird die Service-Aufnahme vorbereitet.

- Der Kunde erhält eine E-Mail mit relevanten Informationen und wird aufgefordert, Informationen und Ansprechpartner (Ziffer 3.1.4), die für eine Bereitstellung und den Betrieb erforderlich sind, zur Verfügung zu stellen. Diese autorisierten Mitarbeiter, die als Ansprechpartner benannt wurden, sind für die aktive Mitarbeit erforderlich.
- Die Telekom richtet für den Kunden einen eigenen Mandanten mit virtuell getrennter Datenhaltung in der Telekom Cloud (multimandantenfähige Plattform) ein. Zusätzlich wird ein Online-Kickoff-Workshop terminiert.
- Innerhalb des Kickoff-Workshops wird u. a. die Verteilung der Endpunkt-Scanner auf die Endpunkte abgestimmt und die Installation durch die Administratoren des Kunden unter Anleitung der Telekom exemplarisch für die ersten Endpunkte durchgeführt.
- Innerhalb des Kickoff-Workshops wird u. a. die Verteilung der Endpunkt-Scanner auf die Endpunkte abgestimmt und die Installation durch die Administratoren des Kunden unter Anleitung der Telekom exemplarisch für die ersten Endpunkte durchgeführt.
- Für den Rollout und die Installation der Endpunkt-Scanner auf seinen Endpunkten ist der Kunde selbst verantwortlich, die Telekom steht bei der Installation beratend zur Seite. Zudem werden die Administratoren des Kunden in die Handhabung der Managementkonsole eingeführt.

- Das System lernt anhand der neuen Daten und ist zunächst nur überwachend aktiv.
- In einem weiteren Online-Workshop werden das Fine Tuning (Beseitigung von zukünftigen Fehlalarmen durch z. B. Whitelisting) vorgenommen sowie die Nutzung weiterer Funktionen (z. B. Auto-Remediation) erklärt und ggf. seine notwendige Einwilligung für die Durchführung automatischer Gegenmaßnahmen eingeholt.
- Abschließend erfolgt die interne Übergabe an das Telekom SOC, welches dann mit der Analyse beginnt und den Kunden bei kritischen Sicherheitsvorfällen informiert. Mit der Übergabe an das Telekom SOC ist der Service vollumfänglich nutzbar. Der Kunde erhält hierzu eine Benachrichtigung per E-Mail.

3.1.3 Nachbestellung von Magenta Security Shield Smart um weitere Endpunkte

Der Kunde kann während der Vertragslaufzeit jederzeit weitere Endpunkte in den Vertrag aufnehmen. Die Vertragslaufzeit läuft in diesen Fällen unverändert weiter. Es besteht dabei jeweils zur Mindestabnahme von 10 Endpunkten. Die Preise für das Onboarding weiterer Endpunkte richten sich nach der Preisliste. Einmalig pro Quartal können die Endpunkte um bis zu 50 Prozent der bisher überwachten Endpunkte, maximal jedoch um 1.000 Endpunkte, ohne zusätzlich Onboardingkosten erhöht werden.

3.1.4 Benennung von Ansprechpartnern

Der Kunde hat, für die Bereitstellung und den Betrieb von Magenta Security Shield Smart, autorisierten Mitarbeiter als Ansprechpartner zu benennen. Die Ansprechpartner sind für die Kommunikation und den Informationsaustausch im Rahmen von Magenta Security Shield Smart verantwortlich und sind im Rahmen des Onboardings (Ziffer 3.1.2) zu benennen sowie während der Vertragslaufzeit aktuell zu halten.

## 3.2 Betrieb

3.2.1 Betrieb der Magenta Security Shield Smart Backend-Plattform

Die Magenta Security Shield Smart Backend-Plattform ist als Software as a Service konzipiert und umfasst die folgenden Leistungen:

- Hosting, Betrieb und Datenhaltung im Telekom-Rechenzentrum
- Zugriffsmöglichkeit auf eine Managementkonsole mit Standard-Reports, die eingesehen und heruntergeladen werden können.

Die Telekom betreibt die Magenta Security Shield Smart Backend-Plattform im Telekom Rechenzentrum durch ihren Unterauftragnehmer. Die betrieblichen Leistungen umfassen insoweit:

- Bereitstellung der Backend-Plattform
- Betrieb und Überwachung der Backend-Plattform
- Support durch das Security Operation Center für Security Incidents (Ziffer 3.4)

3.2.2 Betrieb der Server- und Systemkomponenten

Alle Server- und Systemkomponenten, werden als multimandantenfähige Software as a Service (SaaS) Plattform bereitgestellt. Die Datenhaltung erfolgt mandantengetrennt, wie auch die Zugriffe auf die kundeneigene Managementkonsole. Alle Komponenten werden in einem Rechenzentrum der Telekom innerhalb der Open Telekom Cloud betrieben und haben erfolgreich das obligatorische Telekominterne Sicherheitsaudit (PSA) durchlaufen und sind durch strenge Sicherheitsmaßnahmen geschützt. Die Leistungen zum Betrieb stehen mit einer mittleren Verfügbarkeit von 99,0 % im Kalenderjahr zur Verfügung. Für Betrieb und System-Management gelten folgende Leistungsmerkmale:

- Betriebszeit täglich von 0.00 bis 24.00
- Automatische Erkennung von Störungen

### 3.2.3 Service Qualität

#### 3.2.3.1 Leistungsübergabepunkt

Die Verantwortung der Telekom endet am Leistungsübergabepunkt. Der Leistungsübergabepunkt ist der Eintrittspunkt des Telekom Rechenzentrums ins Internet.

#### 3.2.3.2 Verfügbarkeit des Service

Die Verfügbarkeit der Plattform beträgt mindestens 99 % je Kalenderjahr und wird wie folgt berechnet:

- ((Gesamte Serviceminuten) – (Gesamte Ausfallminuten)) / Gesamte Serviceminuten
- Sie wird als Prozentsatz (Verfügbarkeits-Prozentsatz) ausgewiesen, wobei die Begriffe folgendes bedeuten:
- Gesamte Serviceminuten: Gesamte Anzahl an Minuten innerhalb eines Kalenderjahres (berechnet: 60 Minuten multipliziert mit 24 Stunden mal der Tage im Kalenderjahr).
- Gesamte Ausfallminuten: Anzahl der Minuten innerhalb eines Kalenderjahres, während derer Magenta Security Shield Smart nicht verfügbar war, abzüglich der Minuten für ausgenommene Ereignisse.
- Ausgenommene Ereignisse: Ausfallzeiten aufgrund von ausgenommenen Ereignissen bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt. Das Vorliegen eines ausgenommenen Ereignisses reicht aus.
  - Ausgenommene Ereignisse sind Ausfälle, die durch Wartungsarbeiten oder Changes verursacht wurden, Störungen, Ausfälle und Probleme, die auf den Kunden, seine Mitarbeiter oder Vertreter zurückzuführen sind, oder Ausfälle, die auf eine Einwirkung von Dritten (z. B. DDoS) zurückzuführen sind.

#### 3.2.3.3 Wartungsarbeiten

Die Telekom und deren Unterauftragnehmer führen regelmäßig Wartungsarbeiten durch. Sollten diese Wartungsarbeiten zu Unterbrechungen der Leistung führen, wird die Telekom den Kunden vorab informieren. Die Benachrichtigung erfolgt per E-Mail oder als Meldung in der Kunden-Managementkonsole. Die Telekom ist hierbei bestrebt, Beeinträchtigungen durch Wartungsarbeiten möglichst gering zu halten. Wartungsarbeiten gelten nicht als Ausfallzeiten und bleiben daher bei der Berechnung der Verfügbarkeit unberücksichtigt.

## 3.3 Technischer Support

Der Technische Support für Magenta Security Shield Smart umfasst die Annahme von Störungsmeldungen bzgl. der Backend-Plattform und Endpunkt Scanner, soweit die auftretenden Störungen bei ordnungsgemäßem Gebrauch entstanden sind. Zudem umfasst der Service die Unterstützung des Kunden bei unklaren oder wiederkehrenden Fehlerzuständen in seiner IT-Umgebung, die potenziell durch den Endpunkt-Scanner ausgelöst werden.

### 3.3.1 Störungsannahme technischer Support

Die Telekom nimmt täglich von 0.00 bis 24.00 Uhr Störungsmeldungen des Kunden per E-Mail entgegen.

### 3.3.2 Meldung von Störungen

Die Störungsmeldung des Kunden hat durch die in der Magenta Security Shield Smart Managementkonsole hinterlegten autorisierten Ansprechpartner (Ziffer 3.1.4) zu erfolgen und die folgenden Informationen für die Weiterbearbeitung durch die Telekom zu enthalten:

- Ansprechpartner
- Beschreibung des Vorfalls
- Falls sinnvoll, Quelldaten, wie z. B. Log-Dateien

Es wird empfohlen, die Meldung verschlüsselt an die Telekom zu senden. Erfolgt eine Meldung durch nichtautorisierte Ansprechpartner oder enthält diese nicht die notwendigen Informationen, kann es zur Verzögerung der Bearbeitung

kommen. Die angegebenen Reaktionszeiten werden in diesen Fällen ausgesetzt. Die Kontaktmöglichkeiten zur Meldung von Störungen werden dem Kunden während der Onboarding-Phase mitgeteilt.

#### 3.3.3 Servicebereitschaft

Die Servicebereitschaft ist montags bis freitags in der Zeit von 9.00 bis 17.00 Uhr, sofern diese keine gesetzlichen Feiertage sind.

#### 3.3.4 Reaktionszeit

Die Reaktionszeit ist die Zeit zwischen einer Störungsmeldung durch den Kunden und der Rückmeldung über den Beginn der Aktivitäten der Telekom. Geht die Störungsmeldung während der Servicebereitschaft bis 12.00 Uhr ein, erfolgt die Rückmeldung am gleichen Tag. Ansonsten erfolgt die Rückmeldung spätestens am nächsten Tag der Servicebereitschaft.

#### 3.3.5 Entstörungsfrist

Die Telekom beseitigt die Störung von montags bis freitags (mit Ausnahme von gesetzlichen Feiertagen) innerhalb von 72 Stunden nach Eingang der Störungsmeldung während der Servicebereitschaft. Die Bearbeitung erfolgt innerhalb der Servicebereitschaft. Die Frist ist eingehalten, wenn innerhalb des vereinbarten Zeitraums die Funktionalität wiederhergestellt ist oder dem Kunden ein adäquater Ersatz oder Workaround zur Verfügung gestellt wurde.

#### 3.3.6 Ausnahmen bei softwarebedingten Störungen

Die Telekom ist von der Einhaltung der Servicelevel-Parameter freigestellt, solange der Mangel auf eine softwarebedingte Störung (Bug) zurückzuführen ist und noch keine überarbeitete Softwareversion zur Einspielung von Patches/Updates/Upgrades durch den Unterauftragnehmer bereitgestellt worden ist. Softwarebedingte Störungen sind Störungen, die auf Softwarefehler/Programmierfehler/Konfigurationsfehler zurückzuführen sind.

### 3.4 Support Security Operation Center (SOC)

#### 3.4.1 Annahme von Alarmen

Die Telekom bearbeitet und bewertet täglich von 0.00 bis 24.00 Uhr Security-Alarme, welche durch den Magenta Security Shield Smart Service generiert werden. Die Benachrichtigung des Endkunden erfolgt proaktiv durch das Telekom SOC im Rahmen der Überwachung (Siehe Ziffer 2.3.2). Im Falle von Rückfragen kann sich der Kunde per E-Mail an das Telekom SOC wenden.

#### 3.4.2 Reaktionszeiten des SOC

Im Regelfall empfiehlt die Telekom die Aktivierung automatischer Gegenmaßen. Diese können in Sekundenschnelle auf mögliche Sicherheitsvorfälle reagieren und potenziell gefährliche Situationen unverzüglich entschärfen. Eine zeitaufwendige, tiefe Analyse inklusive Benachrichtigung des Kunden ist somit oftmals nicht mehr nötig. Das Telekom SOC strebt eine schnellstmögliche Analyse und, falls notwendig, Benachrichtigung des Kunden bei einem Sicherheitsvorfall an und priorisiert dabei nach Kritikalität der eingehenden Alarme. Wird der Sicherheitsvorfall als Kritisch eingestuft beträgt der späteste Beginn der Alarmanalyse, ab Alarmeingang, zwei Stunden; eine erste Benachrichtigung erfolgt nach 4 Stunden. Bei einer Einstufung des Sicherheitsvorfalls als Hoch beträgt der späteste Beginn der Alarmanalyse, ab Alarmeingang ebenfalls zwei Stunden und eine Erstbenachrichtigung erfolgt nach acht Stunden.

### 3.5 Optionale Leistungen

Die nachfolgenden optionalen Leistungen werden bei gesonderter Beauftragung gegen zusätzliche Vergütung erbracht. Eine Beratung außerhalb der Lösung Magenta Security Shield Smart, wie z. B. eine Prüfung der bestehenden Kunden-IT-Umgebung auf Sicherheitsbelange sowie jede Form der allgemeinen technischen Sicherheitsberatung gehören nicht zum Leistungsspektrum.

### 3.5.1 Individuelle Beratung

Folgende Leistungen können als Beratungsleistung optional beauftragt werden.

- Zusätzliche Analysetätigkeiten zu Alarmen, Sicherheitsbewertungen (Risk Score) und gesammelten Informationen innerhalb von Magenta Security Shield Smart.
- Unterstützung beim Rollout weiterer Endpunkt-Scanner z. B. bei größeren Änderungen in der Kunden-IT-Umgebung.
- Schulung weiterer autorisierter Ansprechpartner zum Umgang mit der Kunden-Managementkonsole von Magenta Security Shield Smart.
- Kunden, die ein Basispaket ab 501 Endpunkten beauftragt haben, haben maximal eine Stunde Beratung pro Quartal inkludiert. Nicht in Anspruch genommene Beratungsstunden verfallen am Ende des jeweiligen Quartals und werden nicht in das nächste Quartal übertragen.

### 3.5.2 Optionaler Proof of Concept

Um die technische Implementierung und die Leistungsfähigkeit des Tools zu testen, bietet die Telekom dem Kunden optional die Möglichkeit an, die bereitgestellten Tools zu Magenta Security Shield Smart mit Hilfe eines Proof of Concept (PoC) für die weitere Verwendung zu prüfen.

#### 3.5.2.1PoC Leistungen

Abweichend zu den unter dieser Ziffer 3 genannten Leistungen werden im Rahmen des PoC ausschließlich folgende Leistungen erbracht:

- Zwei PoC-spezifische Kundenworkshops (Vorbereitungs- und Abschluss-Workshop)
- Nutzungsberechtigung und Endpunkt-Scanner für maximal dreißig Endgeräte und zwei Wochen Laufzeit
- Technischer Support der Telekom gemäß Ziffer 3.3
- Auf Kundenwunsch: Optionale Erweiterung des PoC für weitere zwanzig Endgeräte und um weitere zwei Wochen Laufzeit gegen gesonderte Vergütung.

#### 3.5.2.2Einrichtung, Ablauf und Durchführung des PoC

Der Magenta Security Shield Smart PoC besteht aus mehreren Aktivitäten, die die Telekom und der Kunde gemeinsam durchführen. Ablauf und Leistungsumfang werden im Folgenden beschrieben:

- Der Kunde erhält eine E-Mail mit Informationen zur Vorbereitung und wird aufgefordert, einen Termin für einen online durchgeführten Vorbereitungsworkshop abzustimmen.
- Die Telekom richtet für den Kunden einen separaten Mandanten mit virtuell getrennter Datenhaltung in der Telekom Cloud (multimandantenfähige Plattform) ein.
- Der Magenta Security Shield Smart PoC beginnt mit dem Vorbereitungsworkshop. Innerhalb des Workshops wird die Installation der Endpunkt-Scanner durch die Administratoren des Kunden unter Anleitung der Telekom exemplarisch für die ersten Endpunkte durchgeführt. Zudem wird der Kunde in die Handhabung der Managementkonsole eingeführt.
- Im weiteren Verlauf werden zusätzliche Details des Produktes, wie Forensik und Schutzmechanismen vorgestellt sowie eine eventuell notwendige Optimierung der Konfiguration (Whitelisting) vorgenommen mit dem Zweck der Aktivierung der automatischen Abwehrfunktionen (Auto-Remediation). Dem Kunden wird die Funktion „Auto-Remediation“ erklärt und darauf hingewiesen, welche Aktionen an den Endpunkten in der Netzumgebung des Kunden ausgeführt werden können und welche Vor- und Nachteile sich durch diese Funktion ergeben. Der Kunde benennt, falls gewünscht, eigenverantwortlich auszuschließende Endpunkte, die keine automatischen Gegenmaßnahmen erfahren. Daraufhin wird der Kunde gebeten, seine Einwilligung für die Durchführung

automatischer Gegenmaßnahmen zu erteilen, im Anschluss wird die Funktion bei vorliegender Einwilligung aktiviert. Damit ist der Kunde auch für die durch diese Funktion automatisch ausgelösten Auswirkungen selbst verantwortlich.

- Danach führt der Kunde den weiteren Rollout der Endpunkt-Scanner auf seinen Endpunkten eigenverantwortlich aus und beginnt mit dem Test des Produktes. Die Telekom steht bei Bedarf beratend zur Seite. Für den Rollout und die Installation der Scanner auf den Kunden-Endpunkten ist der Kunde selbst verantwortlich. In dieser Phase lernt Magenta Security Shield Smart PoC anhand der neuen Daten und ist nur überwachend aktiv.
- Zum Ende des PoC findet ein online durchgeführter Abschluss- Workshop statt, bei dem die Ergebnisse gemeinsam besprochen werden. Hierbei werden Erfahrungen und bisher prüfbare Erfolgskriterien diskutiert.
- Mit dem Abschluss-Workshop endet der PoC. Der Zugang zur Magenta Security Shield Smart Managementkonsole wird beendet.
- Besteht der Wunsch nach einer Beauftragung von Magenta Security Shield Smart, so kann der eingerichtete Mandant maximal vier weitere Wochen vorgehalten werden, um nach Beauftragung mit der Nutzung fortzufahren. Sollte keine Beauftragung von Magenta Security Shield Smart gewünscht sein, ist der Kunde verpflichtet, die Endpunkt-Scanner eigenverantwortlich mit Ende des PoC auf seinen Endpunkten zu deinstallieren. Der Mandant wird durch die Telekom gelöscht.

## 4 Mitwirkungspflichten des Kunden

Der Kunde verpflichtet sich, alle Leistungen, die zur ordnungsgemäßen Leistungserbringung erforderlich sind, insbesondere jedoch nachfolgende, unentgeltlich, rechtzeitig und in erforderlichem Umfang zu erbringen:

- Der Kunde benennt alle Stakeholder, die für eine reibungslose Serviceintegration und einen reibungslosen Servicebetrieb in der Umgebung des Kunden für die Durchführung der Leistungen notwendig sind. Ausschließlich vom Kunden autorisierte Ansprechpartner mit den notwendigen Fachkenntnissen erhalten Zugriff auf die Managementkonsole und müssen sich bei Zugriff authentisieren.
- Der Kunde verpflichtet sich, eine Indikation aller betreffenden Geräte, die zur Überwachung aufzunehmen sind, aufzustellen.
- Der Kunde verpflichtet sich, die Endpunkt-Scanner auf die vereinbarten Systeme innerhalb der eigenen Netzinfrastruktur auszurollen. Der Kunde ist weiterhin für die etwaige Updates der Endpunkt-Scanner in der eigenen Netzinfrastruktur verantwortlich.
- Der Kunde verpflichtet sich, der Anlage eines Mandanten auf der multimandantenfähigen Plattform zuzustimmen und mithilfe zugewiesener Berechtigungen darauf zuzugreifen.
- Der Kunde erkennt an, dass er mit der durch ihn erteilten Einwilligung zu automatisierten und manuellen Gegenmaßnahmen für die Auswirkungen dieser Maßnahmen selbst verantwortlich ist.
- Bei Einwilligung des Kunden zu der Aktivierung der Funktion „Auto-Remediation“ benennt der Kunde eigenverantwortlich die eigenen Endpunkte, bei denen aus geschäftskritischen Gründen diese Funktion nicht zur Ausführung kommen soll.
- Der Kunde verpflichtet sich, sich mit Drittanbietern abzustimmen, falls der für Serviceintegration und Servicebetrieb erforderliche Support vom Drittanbieter zu erbringen ist.
- Der Kunde sichert zu, ausreichend Internetbandbreite und Berechtigungen für die Servicekomponenten vor Ort bereitzustellen, die eine Verbindung mit Servicekomponenten in der Open Telekom Cloud benötigen. Der Bandbreitenanspruch liegt bei 15MB am Tag pro Endpunkt.
- Der Kunde erklärt sich mit dem Schriftwechsel per E-Mail einverstanden und hinterlegt stets eine aktuelle E-Mail-Adresse. Dem Kunden ist bekannt, dass für die Leistungserbringung wesentliche Informationen, wie Zugangsdaten, Informationen zu Änderungen der Leistungen und der rechtlichen Bedingungen ausschließlich per E-Mail versendet

werden. Der Versand sensitiver Daten erfolgt per verschlüsselter E-Mail. Der Kunde erklärt sich bereit, die verschlüsselte E-Mail-Kommunikation mit der Telekom wahrzunehmen.

- Der Kunde ist dafür verantwortlich, alle rechtlichen Bestimmungen, Gesetze, Vorschriften und branchenspezifischen Bestimmungen, die für die Nutzung des Service relevant und anwendbar sind, zu überprüfen und deren Einhaltung sicherzustellen. Dazu gehört insbesondere auch die Einhaltung von Verschwiegenheitspflichten, die beispielsweise von einer beruflichen Tätigkeit herrühren. Der Kunde sichert zu, dass vertrauliche Daten nur verarbeitet werden, nachdem eine gültige Zustimmung eingeholt wurde.
- Der Kunde sichert zu, dass ein qualifizierter Single Point of Contact (SPoC) an allen Workshops während der Onboarding Phase aktiv teilnimmt.
- Der Kunde verpflichtet sich, über Veränderungen in seiner IT-Umgebung, die Auswirkungen auf den Service und die integrierten Datenquellen haben können, zu informieren.
- Der Kunde ist verpflichtet, der Telekom eventuelle Mängel bei der Servicebereitstellung unverzüglich schriftlich per E-Mail an das technische Support-Team zu melden, einschließlich einer nachvollziehbaren Beschreibung der Symptome. Soweit möglich, sollten schriftliche Aufzeichnungen, Papierdokumente oder andere Unterlagen, die die Mängel veranschaulichen, beigelegt werden.
- Der Kunde sichert zu, die Software (Endpunkt-Scanner) zum Ablauf der Überlassungszeit/Vertragslaufzeit auf den Systemen seiner Netzinfrastruktur zu deinstallieren und damit komplett zu entfernen. Eine Nutzung darüber hinaus, darf dem Kunden zu den aktuell gültigen Preisen in Rechnung gestellt werden.
- Der Kunde verpflichtet sich, die Anzahl der eingekauften Endpunktlizenzen einzuhalten. Eine Nutzung darüber hinaus, darf dem Kunden zu den aktuell gültigen Preisen in Rechnung gestellt werden.

# 5 Mindestüberlassungszeit/ Beendigung

Die Mindestüberlassungszeit für Cyber Defense Smart beträgt zwölf Monate und verlängert sich automatisch um weitere zwölf Monate, wenn der Service nicht mit einer Frist von drei Monaten zum Ende der Mindestüberlassungszeit bzw. des jeweiligen Verlängerungszeitraums gekündigt wird. Die Vertragslaufzeit beginnt mit dem Tag der vereinbarten Bereitstellung (Ziffer 3.1) Eine eventuelle Weiternutzung kann erneut beauftragt werden. Mit Beendigung der Leistung werden die Kundendaten gelöscht. Der Kunde kann gemäß Ziffer 3.1.3 während der Vertragslaufzeit weitere Endpunkte in den Vertrag aufnehmen. Die Vertragslaufzeit läuft in diesen Fällen unverändert weiter. Die Kündigung von Endpunkten kann immer nur zum Ablauf der jeweiligen Vertragslaufzeit mit einer Frist von drei Monaten erfolgen. Die Endpunkt-Scanner sind nach Wirksamwerden der Kündigung für den jeweiligen Endpunkt oder den gesamten Vertrag zu deinstallieren und komplett zu entfernen.

# 6 Bedingungen

## 6.1 Zusätzliche Bedingungen zum Datenschutz

Die Leistung von Magenta Security Shield Smart kann nicht erbracht werden ohne die Erhebung und Verarbeitung personenbezogener Daten. Nach der Datenschutz-Grundverordnung (DSGVO) sind sowohl von den Kunden als auch von der Telekom Anforderungen an den gesetzlichen Datenschutz zwingend einzuhalten.

### 6.1.1 Personenbezogene und -beziehbare Daten

Während der Leistungserbringung muss die Telekom personenbezogene und -beziehbare Daten, wie Namen von Benutzerkonten, E Mail-Adressen, IP-Adressen aus den entsprechenden Datenquellen verarbeiten. Die Datenquellen (Endpunkte) werden beim Onboarding mit EndpunktScannern bestückt, damit ihre Protokolldaten zur Verarbeitung an die Servicekomponenten weitergeleitet werden können. Die für den Betrieb der Plattform zuständigen Mitarbeiter der Telekom und des Unterauftragnehmers Cynet Security Ltd. können auf alle übertragenen Daten des Kunden zugreifen, um die Überwachung zu gewährleisten und Analysen in Verdachtsfällen durchzuführen und ggf. Gegenmaßnahmen

einzuleiten. Magenta Security Shield Smart übermittelt grundsätzlich keine besonders schützenswerten personenbezogenen und -beziehbare Daten. Es können jedoch Dateien in einer Sandbox tiefergehend analysiert werden. Da diese Dateien nutzergenerierte Inhalte enthalten können, kann allein der Kunde vor Übertragung der Dateien ausschließen, dass besonders schützenswerte Daten darin enthalten sein können. Daher sollte eine Übertragung von Dateien mit besonders schützenswerten Daten in keinem Falle erfolgen Sofern personenbezogene Daten im Auftrag des Kunden durch die Telekom verarbeitet werden, gelten die ErgB-AV.

#### 6.1.2 Löschung der Daten

Alle Daten, die unter anderem mit Hilfe der Endpunkt-Scanner in der IT-Umgebung des Kunden gesammelt und in das Rechenzentrum der Telekom übertragen werden, werden spätestens nach Ablauf einer Frist von neunzig Tagen ohne Aktualisierung automatisch gelöscht. Dies gilt auch für die Daten von überwachten Endpunkten oder Benutzerkonten die neunzig Tagen inaktiv sind. Nach Kündigung des Vertrags wird der eingerichtete Mandant und die zugehörige Datenbank aus den Backend-Systemen entfernt. Zusätzlich werden Kundendaten in einer mandantenübergreifenden Datenbank gelöscht. Die Löschung der Kundendaten wird spätestens neunzig Tage nach dem wirksam werden der Kündigung des Vertrages abgeschlossen.

### 6.2 Hinweis auf die Rechte Betroffener

Dem Kunden obliegt es, seine Pflichten als verantwortliche Stelle gegenüber Betroffenen im Sinne der Europäischen Datenschutzgrundverordnung zu erfüllen.

#### 6.2.1 Hinweis auf innerbetriebliche Abläufe

Ohne die Erhebung und Verarbeitung personenbezogener Daten kann die Leistung nicht erbracht werden. Nach der Europäischen Datenschutzgrundverordnung sind sowohl vom Kunden als auch von der Telekom Anforderungen an den gesetzlichen Datenschutz zwingend einzuhalten. Im Rechtsverhältnis zwischen dem Kunden und der Telekom wird dies über entsprechende Verträge abgebildet. Im Verhältnis des Kunden zu seinen Mitarbeitern im Betrieb oder in Behörden, in denen das Produkt zum Einsatz gebracht werden soll, sind hierneben auch innerbetriebliche Anforderungen an den Datenschutz und ggf. die Mitbestimmungsrechte zu beachten, die den Einsatz legitimieren. Da die Telekom auf die Einhaltung und Umsetzung der innerbetrieblichen gesetzlichen Anforderungen keinen Einfluss und davon keine Kenntnis hat, weist die Telekom darauf hin, dass die Verantwortung für einen legitimierten Einsatz des Produkts allein im Verantwortungsbereich des Kunden liegt. In Betrieben oder Behörden müssen die Mitbestimmungsrechte bei der Nutzung des Produktes sowie die gültigen gesetzlichen Regeln angewendet werden.

### 6.3 Einseitige Leistungsänderungen

Die Telekom behält sich einseitige Leistungsänderungen und Entgeltreduzierungen zu Gunsten des Kunden vor. Der Kunde erklärt sich mit diesen Anpassungen einverstanden. Die Telekom wird den Kunden über etwaige Anpassungen durch Übersendung aktualisierter Versionen der bestehenden Vertragsunterlagen informieren, welche die bestehenden Unterlagen ersetzen.

## 7 Glossar/ Abkürzungsverzeichnis

| Abkürzung | Beschreibung |
|---|---|
| DDoS | Distributed Denial of Service |
| EDR | Endpoint detection and response |
| IoC | Indicators of Compromise |
| NGAV | Next Generation Anti-Virus |
| SaaS | Software-as-a-Service |

| Abkürzung | Beschreibung |
|---|---|
| SLA | Service Level Agreement |
| SOC | Security Operation Center |
| SPoC | Single Point of Contact |
| UBA | User Behavior Analytics |
| VPC | Virtual Private Cloud |
| Asset | Hosts Dateien Nutzer, Netzwerk (bezogen auf das Produkt) |

www.telekom.de