GESCHÄFTSBEDINGUNGEN 2021

Zahlung
Zahlung netto 30 Tage nach Rechnungsdatum. Die Rechnung wird nach Lieferung der Software/Dienstleistungen versandt.

Gültigkeit der Preise
Die Preise sind 60 Tage lang gültig.

Eigene Nutzung der Software
Die Software erlaubt während der Vertragslaufzeit eine unbegrenzte Anzahl von Empfängern zu Test- und Schulungszwecken entsprechend dem Lizenzmodell (Ausnahme MSSP). Innerhalb der Software gibt es keine Einschränkungen hinsichtlich der Anzahl der erstellten Kampagnen, Domains und Reports. Der Zugang und die Nutzung der LUCY-Produkte, -Dienstleistungen, -Dokumentation und der zugehörigen Materialien sind ausschließlich für die internen Geschäftszwecke der Organisation und nur für die Dauer der Laufzeit Ihres Abonnements gestattet.

Nutzung der Software für Dritte
Die Software kann während der Vertragslaufzeit für das eigene Unternehmen bzw. die rechtlich zugehörigen Gesellschaften genutzt werden. Dazu gehören auch Unternehmen, an denen der Kunde mehrheitlich beteiligt ist oder die ihm rechtlich gehören, die er direkt oder indirekt kontrolliert oder deren Geschäftsführung mehrheitlich nachgewiesen werden kann.

Lieferung der Dienstleistung/Software
Die Erstellung eines Lizenzschlüssels setzt eine bestehende Installation voraus. Der Kunde kann die Software jederzeit kostenlos von unserer Website herunterladen oder einen Cloud-Server bei LUCY anfordern. Lucy Security AG gewährt den Zugriff auf die lizenzierten Funktionen innerhalb von maximal 5 Tagen nach Bestelleingang. Der Kunde benötigt dazu die an uns zu liefernde Workstation-ID. Diese ID befindet sich im Administrationsbereich unter Support/Lizenzen.

Software-Garantie
Lucy Security AG gewährleistet, dass die Software während der Nutzung der Software durch den Käufer (i) frei von Viren, Malware, Spyware oder sonstigem Softwarecode* ist, der eine Gefahr für die IT-Infrastruktur des Käufers und der mit ihm verbundenen Unternehmen darstellen kann, und (ii) ist frei von Mängeln und Fehlern (mit Ausnahme von geringfügigen Fehlern, die keinen Einfluss auf die Funktionalität der Software haben), und (iii) stellt kein Sicherheitsrisiko für die IT-Umgebung des Käufers und seiner verbundenen Unternehmen dar, und (iv) verletzt keine Rechte Dritter, und (v) verstößt nicht gegen Gesetze. Geringfügige Fehler (sog. Bugs) werden so schnell wie möglich behoben, spätestens jedoch innerhalb von 1 Monat nach Meldung *Die Software enthält eine Funktion, die die Funktionsweise und das Verhalten eines Virus simulieren kann. Der Käufer ist dafür verantwortlich, diese und alle anderen Funktionen der Software in Übereinstimmung mit den lokalen Gesetzen (z.B. Datenschutz für gesammelte Ergebnisse) zu nutzen. Im Falle eines Verstoßes gegen eine der Garantien wird Lucy Security AG den Käufer und seine verbundenen Unternehmen in vollem Umfang verteidigen, entschädigen und von jeglichen Verlusten, Verbindlichkeiten, Schäden, Ansprüchen, Kosten und Ausgaben freistellen. Lucy Security AG gewährleistet, dass alle notwendigen Maßnahmen* getroffen wurden, um einen Missbrauch der Software durch Dritte zu verhindern, der ein Sicherheitsrisiko für die IT-Infrastruktur des Käufers darstellen würde *Es liegt in der Verantwortung des Käufers, ein sicheres Passwort zu setzen, um den Zugang zu LUCY zu schützen.

Beschränkung der Haftung
Außer im Falle einer Verletzung eines geistigen Eigentumsrechts einer Partei, die zu Schadensersatzpflichten führt, und/oder eines Verstoßes gegen geltende Datenschutzgesetze (einschließlich, aber nicht beschränkt auf die GDPR) sowie des Datenverarbeitungszusatzes durch LUCY, haftet eine Partei nicht für besondere, zufällige, Folge- oder exemplarische Schäden jeglicher Art, einschließlich, aber nicht beschränkt auf entgangenen Gewinn und entgangene Einsparungen, unabhängig davon, wie sie verursacht wurden. Die hierin enthaltenen Beschränkungen und Ausschlüsse beschränken sich auf das nach geltendem Recht maximal zulässige Maß. LUCY verpflichtet sich, den Kunden in Bezug auf alle Ansprüche, Haftungen und Schäden, für die der Kunde im Zusammenhang mit einem Verstoß gegen geltende Datenschutzgesetze (einschließlich, aber nicht beschränkt auf die GDPR) sowie den Zusatz zur Datenverarbeitung haftbar gemacht wird, zu entschädigen und schadlos zu halten.

Lizenzdauer
Jede Software wird für den in der jeweiligen Bestellung angegebenen Zeitraum lizenziert. Sofern in der Bestellung nicht anders angegeben, verlängert sich die Softwarelizenz automatisch über die ursprüngliche Laufzeit der Softwarelizenz hinaus um 12 Monate. Software-Supportleistungen werden für den in der jeweiligen Bestellung angegebenen Zeitraum erbracht, oder, falls kein Zeitraum für Supportleistungen angegeben ist, werden Supportleistungen für einen Zeitraum von einem (1) Jahr ab dem Datum der Lieferung der Software an den Kunden erbracht. Nach Ablauf der kommerziellen Lizenz ist die LUCY-Software automatisch als "Community Edition" verfügbar. Der Administrator hat weiterhin Zugriff auf alle Inhalte (E-Learnings oder Angriffsvorlagen), aber der Zugang zu anderen Funktionen ist eingeschränkt. Der volle Funktionsumfang der Software kann jederzeit durch den Erwerb eines neuen Lizenzschlüssels wiederhergestellt werden.

Kündigung der Lizenz
Die Lizenz muss 30 Tage vor dem Ablaufdatum gekündigt werden.

Auswirkung der Kündigung
Bei Beendigung einer SOW oder einer Bestellung, gleich aus welchem Grund, erlöschen alle hierin gewährten Zugriffsrechte und Lizenzen in Bezug auf die betroffene Bestellung oder SOW sofort. Die Beendigung oder der Ablauf eines Auftrags oder einer SOW gilt nicht als Beendigung oder Ablauf eines anderen Auftrags oder einer SOW, der/die zum Zeitpunkt der Beendigung oder des Ablaufs in Kraft ist, und diese Vereinbarung gilt weiterhin für solche ausstehenden Aufträge und SOWs, bis diese Aufträge und SOWs durch ihre eigenen Bedingungen oder wie hierin festgelegt abgelaufen oder beendet sind. LUCY

Security AG | Adresse: Chamerstrasse 44, 6300 Zug, Schweiz |Tel: +41 44 557 19 37| Web: www.lucysecurity.com |Mail: info@lucysecurity.com | Twitter https://twitter.com/lucysecurity

Professionelle Dienstleistungen
Die Leistungsfrist für Professional Services beginnt mit dem in der jeweiligen Bestellung angegebenen Datum oder, falls zwischen den Parteien schriftlich anders vereinbart, mit der in der jeweiligen Bestellung angegebenen Dauer. Ist in der Bestellung keine Frist für die Erbringung von Professional Services angegeben, beginnen die Professional Services mit dem Inkrafttreten des SOW und dauern bis zu dessen Abschluss, sofern in der Bestellung nichts anderes angegeben ist.

Datenschutz & GDPR
Lucy Security AG verpflichtet sich zur Einhaltung der anwendbaren Datenschutzbestimmungen gemäß einem separaten Datenverarbeitungszusatz, der von den Parteien abgeschlossen wird. Zur Einhaltung der lokalen Datenschutzgesetze ist der Kunde für die Auswahl der entsprechenden LUCY-Einstellungen verantwortlich. LUCY Security hat sich zur Einhaltung der in der EU geltenden GDPR-Richtlinien verpflichtet. Anfragen und Anträge bezüglich der Datenschutzrechte des Kunden sollten an dpo@lucysecurity.com gesendet werden. Innerhalb von zehn (10) Werktagen nach Beendigung dieser Vereinbarung oder auf schriftliche Aufforderung des Offenlegers wird LUCY alle vertraulichen Informationen des Offenlegers, die sich im Besitz von LUCY oder eines Vertreters von LUCY befinden, unverzüglich vernichten oder zurückgeben.

Support
Alle Supportleistungen im Zusammenhang mit Softwarefehlern sind kostenlos. Der Stundensatz für Supportleistungen beträgt $90. Support-Rechnungen werden monatlich oder jährlich erstellt. Alle ausgestellten Rechnungen sind innerhalb von dreißig (30) Tagen nach Rechnungsdatum fällig und zahlbar. Andere Ausnahmen: Wenn ein WIKI-Artikel nicht eindeutig formuliert oder veraltet ist, werden dem Kunden die daraus resultierenden Fragen nicht in Rechnung gestellt. Alle anderen Fragen werden in Rechnung gestellt, sobald das im jeweiligen Lizenzmodell enthaltene Support-Budget aufgebraucht ist. Bitte stellen Sie sicher, dass die LUCY-Software immer auf dem neuesten Stand ist, bevor Sie unseren Kundendienst kontaktieren. Nichtsdestotrotz ist das LUCY-Team stets bemüht, hilfsbereit und zuvorkommend zu sein, und wird sein Bestes tun, um dem Kunden zu helfen, wo immer es möglich ist. Beispiele für Probleme, die nicht als LUCY-Fehler angesehen werden:

- Anwendungs- oder Systemprobleme, die durch Änderungen innerhalb des Linux-Betriebssystems, auf dem LUCY läuft, verursacht werden.
- SPAM-Filter von Drittanbietern, die Mails von LUCY blockieren.
- Externe Mail-Relays, die nicht wie erwartet funktionieren.
- Proxy-Einstellungen, die LUCY daran hindern, Updates zu empfangen
- DNS-Konfigurationsprobleme, die durch nicht von LUCY vorgenommene DNS-Einträge verursacht werden.

Sicherheit und Überwachung in der LUCY VPS/SaaS Umgebung
Die folgenden Informationen beschreiben den Prozess der Installation und Unterstützung eines neuen LUCY-Servers, wenn dieser von LUCY gehostet wird. Im Falle des Erwerbs der SaaS-Edition erstellt LUCY einen neuen Server auf der Infrastruktur des von LUCY bevorzugten Providers im Land der Wahl des Kunden (standardmässig sind die Server in Deutschland bei Hetzner.com) Sobald der LUCY-Server erstellt ist, wird die Sicherheitssoftware verteilt, installiert und konfiguriert, wobei das Playbook Ansible im automatisierten Modus verwendet wird. Die zentralisierte Installation und Konfiguration der Sicherheitssoftware ermöglicht eine einheitliche Automatisierung für die schnelle Installation und Konfiguration eines beliebigen Servers. Nach der Installation der Schutz-Tools wird das System mit dem Lynis-Tool überprüft. Die Schutzwerkzeuge von LUCY Server bestehen aus den folgenden Komponenten:

- Alle LUCY-Server haben eine konfigurierte Firewall, um den Zugang zu den Servern zu beschränken. Der Zugang ist nur für den Systemadministrator und das Support-Team erlaubt. Bei Bedarf kann der Zugang (root) auch exklusiv dem Client zugewiesen werden.
- Der Fail2ban-Daemon läuft zum Schutz vor Brute-Force-Angriffen und ist so konfiguriert, dass er sowohl SSH als auch Postfix schützt.
- Der Auditd-Daemon liefert detaillierte Informationen über alle Systemereignisse, insbesondere Informationen über Sicherheitsverletzungen, die es ermöglichen, die notwendigen Maßnahmen zu ergreifen. Die Ereignisinformationen sind in lokal gespeicherten Protokolldateien verfügbar.
- Lynis - ein flexibles Tool, das normalerweise nach der Installation eines neuen Servers ausgeführt wird und es ermöglicht, ein neues System auf folgende Weise zu überprüfen: Sicherheitsaudits, Compliance-Tests, Penetrationstests, Schwachstellenerkennung und Systemhärtung.
- Rkhunter - wird wöchentlich ausgeführt und dient dazu, den Server auf Rootkits, Backdoors und mögliche lokale Exploits zu scannen. Die Scanergebnisse sind in lokal gespeicherten Protokolldateien verfügbar.
- Zabbix-Agent - wird zur Überwachung von Prozessen und Hardware auf dem LUCY-Server verwendet.
- Backup-Skript - wird für die Verschlüsselung von LUCY-Backups und die Übertragung von Backups auf den Backup-Server verwendet. Wenn Sie keine externen Backups benötigen, können wir diese Funktion deaktivieren.

Zusätzlich laufen Zabbix-Agenten im 24×7-Modus auf allen LUCY-Servern. Sie dienen der Überwachung von Prozessen und Dämonen, die für den erfolgreichen Betrieb von LUCY erforderlich sind. Die Zabbix-Agenten halten die Verbindung zum zentralen, eigenständigen Zabbix-Server aufrecht und melden alle wichtigen Ereignisse an diesen. Der Zabbix-Server sendet im Falle von Problemen Alarm-E-Mails an den Systemadministrator und an das Support-Team. Basierend auf den Überwachungsalarmen reagiert der Systemadministrator oder das Support-Team sofort auf jedes gefundene Problem, z. B. Serverabsturz, Nichtverfügbarkeit des Netzwerks, unzureichender Speicherplatz, etc. Bei der Installation von LUCY auf einem dedizierten Server mit RAID überwacht der Zabbix-Agent auch den Status des RAID-Arrays, um einen möglichen Datenverlust aufgrund von Festplattenfehlern zu verhindern. Elk Stack und Wazuh Software ermöglichen die Echtzeit-Überwachung von möglichen Schwachstellen in den verwendeten LUCY-Komponenten. Elk Stack und Wazuh Software werden auch für bestimmte Vorfallstypen verwendet. Basierend auf dem Vorfallstyp werden spezifische Regeln für den Eskalationsprozess definiert. Elk Stack und Wazuh Software ermöglichen eine Echtzeit-Überwachung von möglichen Schwachstellen in den verwendeten LUCY-Komponenten. Elk Stack und Wazuh Software werden auch für bestimmte Vorfallstypen verwendet. Basierend auf dem Vorfallstyp werden spezifische Regeln für den Eskalationsprozess definiert. Elk Stack und Wazuh Software

werden auch für bestimmte Vorfallstypen verwendet. Je nach Art des Vorfalls werden spezifische Regeln für den Eskalationsprozess festgelegt. Da die Aktualisierung auf die neue Version von LUCY nur möglich ist, wenn alle Kampagnen gestoppt sind, wird der Aktualisierungsprozess der LUCY-Software nach der Veröffentlichung einer neuen LUCY-Version manuell vom Kunden durchgeführt. Die Aktualisierung kann mit einem Klick auf eine Schaltfläche durchgeführt werden.

Datenbank-Verschlüsselung
LUCY speichert alle zugehörigen Daten in PostgreSQL 9.6 RDBMS. Alle dort gespeicherten sensiblen Informationen sind verschlüsselt, da PostgreSQL nur für interne Verbindungen verfügbar ist. Es gibt keine konfigurierbaren Optionen für die DB-Verschlüsselung. Die Verschlüsselung ist für alle Daten obligatorisch und wird automatisch mit den folgenden Einstellungen durchgeführt:

- Es handelt sich um eine Verschlüsselung auf Spaltenebene, die sowohl auf der Anwendungs- als auch auf der DB-Ebene durchgeführt wird, bevor Daten in der Datenbank gespeichert werden. Wir verwenden keine TDE (transparente Datenbankverschlüsselung), da PostgreSQL diese nicht unterstützt, daher verschlüsseln wir nur eine Teilmenge der Spalten in der DB - alles, was kunden-/angriffs-/empfängerbezogene Daten enthält.
- Meistens führen wir die Ver-/Entschlüsselung auf der Anwendungsebene durch, aber es gibt bestimmte Abfragen, die Daten aus Bequemlichkeit auf der DBMS-Ebene entschlüsseln - zum Sortieren und zur Datensuche.
- Die Verschlüsselung wird mit AES-256-CBC durchgeführt.
- Auf Wunsch können wir eine HSM-Lösung anbieten, die es uns ermöglicht, eine HSM-basierte Verschlüsselung zu verwenden - in diesem Fall wird der Verschlüsselungsschlüssel auf dem externen Hardwaremodul mit Manipulationssicherung gespeichert.

Vertraulichkeitsverpflichtungen
Für die Zwecke dieser Vereinbarung bezeichnet der Begriff "vertrauliche Informationen" alle nicht öffentlichen Informationen, einschließlich, aber nicht beschränkt auf technische, Entwicklungs-, Marketing-, Verkaufs-, Betriebs-, Leistungs-, Kosten-, Know-how-, Geschäftspläne, Geschäftsmethoden und Prozessinformationen, die dem Empfänger offengelegt werden. Der Einfachheit halber kann die offenlegende Partei schriftliche vertrauliche Informationen mit dem Vermerk "Vertraulich" oder einer gleichwertigen Bezeichnung kennzeichnen, ist aber nicht dazu verpflichtet. Alle vertraulichen Informationen, die dem Empfänger offengelegt werden, sind ausschließlich für den Geschäftszweck und für keinen anderen Zweck zu verwenden. Der Empfänger verpflichtet sich, die vertraulichen Informationen der offenlegenden Partei vertraulich zu behandeln und die Vertraulichkeit dieser vertraulichen Informationen mit demselben Maß an Sorgfalt zu schützen, mit dem er die Vertraulichkeit seiner eigenen vertraulichen Informationen schützt, jedoch keinesfalls mit weniger als einem angemessenen Maß an Sorgfalt. Der Empfänger darf vertrauliche Informationen nur an seine Angestellten, Bevollmächtigten, Berater und Auftragnehmer weitergeben, wenn diese davon Kenntnis haben müssen, und nur dann, wenn diese Angestellten, Bevollmächtigten, Berater und Auftragnehmer entsprechende schriftliche Vereinbarungen mit dem Empfänger abgeschlossen haben, die es dem Empfänger ermöglichen, alle Bestimmungen dieser Vereinbarung durchzusetzen. Der Empfänger darf keine Kopien der vertraulichen Informationen der offenlegenden Partei anfertigen, es sei denn, sie werden für den Geschäftszweck benötigt. Auf Verlangen der Offenlegenden Partei ist der Empfänger verpflichtet, der Offenlegenden Partei alle vertraulichen Informationen der Offenlegenden Partei (einschließlich aller Kopien davon) zurückzugeben oder deren Vernichtung zu bescheinigen. Alle Rechte, Titel und Interessen an den vertraulichen Informationen verbleiben bei der offenlegenden Partei oder ihren Lizenzgebern. Die hier dargelegten Verpflichtungen und Beschränkungen in Bezug auf vertrauliche Informationen gelten nicht für Informationen, die: (a) zu irgendeinem Zeitpunkt öffentlich zugänglich sind, es sei denn, der Empfänger hat gegen die Geheimhaltungspflicht verstoßen; oder (b) zu irgendeinem Zeitpunkt rechtmäßig von einem Dritten erhalten wurden, der das Recht dazu hatte und sie ohne Geheimhaltungspflicht an den Empfänger weitergibt. Verstößt der Empfänger gegen diese Vereinbarung oder scheint ein Verstoß unmittelbar bevorzustehen, hat die offenlegende Partei Anspruch auf alle ihr gesetzlich zustehenden Rechtsbehelfe und kann darüber hinaus alle angemessenen Kosten und Anwaltshonorare geltend machen, die ihr bei der Durchsetzung dieser Rechtsbehelfe entstehen. Werden die vertraulichen Informationen von einem Dritten angefordert, auch durch eine Vorladung oder ein sonstiges gerichtliches Verfahren, so hat der Empfänger die offenlegende Partei so rechtzeitig von dem Ersuchen zu unterrichten, dass die offenlegende Partei Einspruch erheben und erforderlichenfalls ein gerichtliches Verfahren einleiten kann, um die Offenlegung zu verhindern.

Anwendbares Recht und Streitbeilegung
Dieser Vertrag unterliegt dem schweizerischen Recht. Für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag sind die zuständigen Gerichte in Zürich zuständig. Allfällige vorhergehende Geschäftsbedingungen der Lucy Security AG werden vollumfänglich wegbedungen und werden nicht Bestandteil dieses Vertrages, es sei denn, der Kunde hat solche allgemeinen Geschäftsbedingungen ausdrücklich schriftlich akzeptiert.