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

TERMS AND CONDITIONS 2021

Payment
Payment net 30 days after invoice date. Invoice is sent after delivery of software/services.

Price Validity
Prices are valid for 60 days

Own use of the Software
The Software allows an unlimited number of recipients for testing and training during the contractual period according to the license model (exception MSSP). There are no restrictions within the Software regarding the number of campaigns, domains and reports created. Access and use of the LUCY products, services, documentation and related materials are solely authorized for the internal business purposes of the organization in which you are a representative of and only for the duration of the term of your subscription period.

Use of the Software for third parties
The Software can be used during the contract period for your own organization. This also includes companies in which the customer has a majority shareholding or legally belongs, which the customer controls directly or indirectly or has the power to appoint/ remove a majority of its management.

Delivery of Service/Software
The creation of a license key requires an existing installation. The customer can download the Software from our website at any time free of charge or request a cloud server from LUCY. Lucy Security AG grants access to the licensed functions within a maximum of 5 days after receipt of the order. The customer needs the workstation ID to be delivered to us. This ID is located in the administration area under support/license.

Software Warranty
Lucy Security AG warrants that during the use of the Software by the buyer the Software (i) is free from any virus, malware, spyware or any other software code* that may pose a danger to the buyer and its affiliates' IT infrastructure, and (ii) is free from any defects and errors (except for minor errors that have no impact on the functionality of the Software), and (iii) does not create any safety risk to the buyer and its affiliates' IT environment, and (iv) does not violate any third party rights, and (v) does not violate any laws. Minor errors (so-called bugs) are being fixed as fast as possible but within a period of 1 month after reporting latest *The Software contains a feature which can simulate the functionality and behavior of a virus. The buyer is responsible to use this and all other features of the Software in accordance of local laws (e.g. data privacy for collected results). In the event of breach of any of the warranties, Lucy Security AG shall fully defend, indemnify and hold the buyer and its affiliates harmless from any against any loss, liabilities, damages, claims, costs and expenses. Lucy Security AG warrants that all necessary measures* have been implemented to avoid any abuse of the Software by any third party which would pose a safety risk to the buyer's IT infrastructure *It is the buyer's responsibility to set a secure password to secure the access to LUCY.

Limitation of Liability
Effect of terminationExcept in the case of 1) a breach of a right of intellectual property of a party which results in compensation obligations and/ or 2) a breach of applicable data protection laws (including, but not limited to the GDPR) as well as the Data Processing Addendum by LUCY, a party shall not be liable for any special, incidental, consequential or exemplary damages of any kind, including but not limited to lost profits and lost savings, regardless of how they were caused. The limitations and exclusions contained herein are limited to the maximum extent permitted by applicable law. LUCY agrees to indemnify and hold harmless Customer in relation to any and all claims, liabilities, damages which the Customer becomes liable for in relation to any breach of applicable data protection laws (including, but not limited to the GDPR) as well as the Data Processing Addendum.

License period
Each Software is licensed for the period specified in the particular order. Unless otherwise specified in the order, the Software License will be automatically extended beyond the initial term of the Software License for 12 months.

Software support services will be provided for the period specified in each order, or, if no period for support services is specified, support services will be provided for a period of one (1) year from the date of delivery of the Software to the Customer Customers provided. Once the commercial license has expired, the LUCY software is automatically available as "Community Edition". The administrator will still have access to all content (e-learnings or attack templates), but access to other functions will be restricted. The full functionality of the Software can be recovered at any time by purchasing a new license key.

License cancellation
The license needs to be cancelled 30 days prior to expiry date.

Effect of termination
Upon termination of any applicable SOW or Order for any reason, all access rights and licenses granted herein in respect of the affected Order or SOW will cease immediately. The termination or expiration of any order or SOW shall not be deemed termination or expiration of any other order or SOW in effect at the time of termination or expiration, and this Agreement shall continue to apply to such outstanding orders and SOWs until such orders and SOWs have expired or terminated by their own terms or as set forth herein. LUCY Security AG | Address: Chamerstrasse 44, 6300 Zug, Switzerland |Tel: +41 44 557 19 37| Web: www.lucysecurity.com |Mail: info@lucysecurity.com | Twitter https://twitter.com/lucysecurity

Professional services
The period of performance for Professional Services begins with the date specified in the applicable order or, as otherwise agreed between the parties in writing, and remains in effect for the duration specified in the applicable order. If the applicable order does not specify a time limit for Professional Services, then professional services commence upon the entry into force of SOW and continue until completed unless otherwise stated herein.

Data Protection & GDPR
Lucy Security AG undertakes to comply with applicable data protection rules according to a separate Data Processing Addendum to be entered into by the parties. To comply with local data protection law, the client is responsible selecting the according LUCY settings. LUCY Security has committed itself to comply with the GDPR guidelines applicable in the EU. Inquiries and requests regarding the customer's data protection rights should be sent to dpo@lucysecurity.com. Within ten (10) business days of the termination of this Agreement or upon Discloser's written request, LUCY will promptly destroy or return all of Discloser's Confidential Information in LUCY's possession or in the possession of any representative of LUCY

Support
All support activities related to software bugs are free of charge. The hourly price for support services is $90. Support bills will be created monthly or yearly. All invoices issued hereunder are due and payable within thirty (30) days of the invoice date. Other exceptions: If a WIKI article is not clearly formulated or is outdated, the customer will not be charged for the resulting questions. All other issues will be charged once the support budget included in the according license model is used up. Please ensure that the LUCY software is always up to date with the latest patch before contacting our customer service. Having said all that, the LUCY team aims to be helpful and accommodating at all times, and will do its absolute best to assist the client wherever possible. Examples of issues that are not considered LUCY bugs:

- Application or system problems caused by changing anything within the Linux operating system on which LUCY runs.
- Third party SPAM filters blocking mails from LUCY.
- External Mail relays that do not work as expected.
- Proxy settings preventing LUCY to receive updates
- DNS configuration issues caused by DNS entries not made by LUCY.

Security and Monitoring on LUCY VPS/SaaS environment
The following information describes the process of installing and supporting a new LUCY server when it is hosted by LUCY. In case of purchasing the SaaS edition, LUCY creates a new server on the infrastructure of LUCY's prefered provider in the country of the customer's choice (by default the servers are setup in Germany at Hetzner.com). Once the LUCY server is created, security software is distributed, installed and configured using Playbook Ansible in automated mode. Centralized installation and configuration of the security software allows us to achieve the unified automation for rapid installation and configuring of any server. After the installation of the protection tools, the system check is performed using Lynis tool. LUCY server's protection tools consists oft he following components:

- All LUCY serves have configured Firewall to restrict access to the servers. The access is only allowed for the System Administrator and Support team. If required, access (root) can also be assigned exclusively to the client.
- Fail2ban daemon is running for protection from brute-force attacks, it is configured to protect both SSH and Postfix.
- Auditd daemon provides the detailed information about all system events, especially information on security violations that allows to take necessary actions. The event information is available in log files stored locally.
- Lynis – a flexible tool that is normally executed after installation of a new server and allows to check a new system in the following ways: Security audits, Compliance testing, Penetration testing, Vulnerability detecting & System hardening.

- Rkhunter – is executed weekly, it is used to scan the server for rootkits, backdoors and possible local exploits. The scanning results are available in log files stored locally.
- Zabbix agent – is used for monitoring processes and hardware on the LUCY server.
- Backup script – is used for encrypting LUCY backups and transferring backups to the backup server. If you do not require external backups, we can disable this feature.

Additionally, Zabbix agents are running in 24×7 mode on all LUCY servers. They are used for monitoring processes and daemons required for successful operation of LUCY. Zabbix agents keep connection to central stand-alone Zabbix server and report all important events to it. Zabbix server send alarm e-mails to System Administrator and to Support team in case of problems. Based on monitoring alarms System Administrator or Support team immediately react to any problem found, e. g. server crash, network unavailability, insufficient disk space, etc. In case of installation LUCY on a dedicated server with RAID Zabbix agent also monitors the status of the RAID array in order to prevent possible data loss due to hard disk malfunctioning. Elk stack and Wazuh Software allow real-time monitoring of possible vulnerabilities in the used LUCY components. Elk stack and Wazuh Software are also used for certain incident types. Based on the incident type, specific rules for escalation process are defined. Elk stack and Wazuh Software allow real-time monitoring of possible vulnerabilities in the used LUCY components. Elk stack and Wazuh Software are also used for certain incident types. Based on the incident type, specific rules for escalation process are defined. Elk stack and Wazuh Software are also used for certain incident types. Based on the incident type, specific rules for escalation process are defined. Patches to the OS (Debian) are automatically rolled out using the software “Patchman” Since updating to the new version of LUCY is only possible when all campaigns are stopped, the LUCY software updating process is done manually by the client after publishing a new LUCY version. The update can be done with a click of a button.

Database Encryption

LUCY stores all related data in PostgreSQL 9.6 RDBMS. All sensitive information stored in there is encrypted as PostgreSQL is available only for internal connections. There are no configurable options for the DB encryption. The encryption is mandatory for all data and is performed automatically with the following settings:

- It’s a column-level encryption performed on both the application and DB layers before storing any data in the database. We don’t use TDE (transparent database encryption), as PostgreSQL doesn’t support it, so we encrypt only a subset of columns in DB – everything that holds client/attack/recipient-related data.
- We mostly perform the encryption/decryption on the application level, but there are certain queries that decrypt data on the DBMS level for convenience – for sorting & data search.
- The encryption is performed using AES-256-CBC.
- On demand we can provide a HSM solution, that will allow us to use a HSM-based encryption – in that case the encryption key will be stored on the external hardware module with anti-tampering protection.

Confidentiality Obligations

For purposes of this Agreement, "Confidential Information" shall mean any and all non-public information, including, without limitation, technical, developmental, marketing, sales, operating, performance, cost, know-how, business plans, business methods, and process information, disclosed to the Recipient. For convenience, the Disclosing Party may, but is not required to, mark written Confidential Information with the legend "Confidential" or an equivalent designation. All Confidential Information disclosed to the Recipient will be used solely for the Business Purpose and for no other purpose whatsoever. The Recipient agrees to keep the Disclosing Party’s Confidential Information confidential and to protect the confidentiality of such Confidential Information with the same degree of care with which it protects the confidentiality of its own confidential information, but in no event with less than a reasonable degree of care. Recipient may disclose Confidential Information only to its employees, agents, consultants and contractors on a need-to-know basis, and only if such employees, agents, consultants and contractors have executed appropriate written agreements with Recipient sufficient to enable Recipient to enforce all the provisions of this Agreement. Recipient shall not make any copies of Disclosing Party’s Confidential Information except as needed for the Business Purpose. At the request of Disclosing Party, Recipient shall return to Disclosing Party all Confidential Information of Disclosing Party (including any copies thereof) or certify the destruction thereof. All right title and interest in and to the Confidential Information shall remain with Disclosing Party or its licensors. The obligations and limitations set forth herein regarding Confidential Information shall not apply to information which is: (a) at any time in the public domain, other than by a breach on the part of the Recipient; or (b) at any time rightfully received from a third party which had the right to and transmits it to the Recipient without any obligation of confidentiality. In the event that the Recipient shall breach this Agreement, or in the event that a breach appears to be imminent, the Disclosing Party shall be entitled to all legal and equitable remedies afforded it by law, and in addition may recover all reasonable costs and attorneys' fees incurred in seeking such remedies. If the Confidential Information is sought by any third party, including by way of subpoena or other court process, the Recipient shall inform the Disclosing Party of the request in sufficient time to permit the Disclosing Party to object to and, if necessary, seek court intervention to prevent the disclosure.

Applicable law and dispute resolution

This contract shall be governed by Swiss law. Any dispute arising out of or in connection with this contract shall be brought before the competent courts in Zurich. Any pre-printed terms and conditions of Lucy Security AG shall be excluded in their entirety and shall not become part of this contract, unless and to the extent that the client has explicitly accepted in writing such general terms and conditions