Offensity Security Monitoring & Reporting

Service description

Version: 4.0

Date: 13 Dec. 2019

Table of Contents

1 General Information

The German version of this service description is the only legally binding version (https://www.a1.digital/at/ueber-a1-digital/agbs/) – any translations, including this English version, are to be considered as information only!

This service description applies starting 13 Dec. 2019. It details the characteristics of all Offensity Security Monitoring ("Offensity" for short") offered and provided to you as a customer of A1 Digital International GmbH ("A1 Digital" for short). Unless otherwise agreed here in writing, the General Terms and Conditions for Cloud and Software Solutions of A1 Telekom Austria AG shall apply mutatis mutandis.

All Offensity applications are cloud-based services which can be used from any location. The customers receive the necessary login credentials for the duration of the selected subscription (monthly, annual).

Only contractors as defined in § 1 of the Konsumentenschutzgesetz (KSchG (Consumer Protection Act)) can be Offensity service customers.

2 Applications

Offensity helps companies that want to take technical measures in accordance with the state-of-the-art to detect vulnerabilities on an ongoing basis in order to secure their externally accessible IT systems. Recording all identified risks in a standardised manner and solution-oriented reports reduce the customer's response time and make it possible to document and prioritise the measures to be implemented.

A1 Digital does not assume any responsibility for all existing vulnerabilities being detected. Depending on the selected configurations, it is, for instance, always possible that individual systems or vulnerabilities might be overlooked.

Offensity includes the following applications: Domain-based asset discovery, vulnerability scans and risk assessment and solution-oriented reports. The vulnerabilities and data sets detected by Offensity are treated confidentially.

2.1 Domain-based asset discovery

Based on the customer's domain name (e.g. example.com"), corresponding, externally accessible IT systems are surveyed. This includes, for instance, DNS and email servers as well as subdomains.

2.1.1 Domain control validation

When the domain is activated, customers can currently choose between the following three "state-of-the-art" technical methods by which Offensity verifies their domain ownership:

- **Email-based domain control validation**: When the order is placed, an email address is selected from a shortlist of acceptable options. An email is sent to that address, containing a unique validation code. The email should be received by someone in control of the domain. The list of acceptable email addresses for any given domain are, for instance, admin@, administrator@, hostmaster@, postmaster@, or any

administrator, registrant, tech or zone contact email address that appears on the domain's WHOIS record[1], and is visible to us.
- **DNS-based domain control validation**: The registrant has to upload a predefined text code as a so-called DNS text record in his DNS management console.
- **HTTP-based domain control validation**: The registrant has to upload an authentication file to the root folder of his website.

2.2 Vulnerability scans and risk assessment

The systems are examined on the network side, from the Internet, with the help of security scanners and automated analyses to obtain information that an attacker can use to prepare and execute virtual break-ins. The tools used currently check known vulnerabilities in network components, operating systems, applications and protocols if they can be verified from the Internet. They are evaluated in the framework of an automated risk analysis. The risk status is documented and can be compared with past results at any time. When new vulnerabilities are found, the customer infrastructure will be checked for susceptibility depending on the technical options, feasibility, risk potential and relevance.

The customer shall ensure that the systems used for vulnerability scans are excluded from dynamic security restrictions (e.g. web application firewalls, fail2ban, etc.). A exception from static security measures (such as a packet filtering firewall) is possible, but A1 Digital does not recommend it.

The source systems and their IP address ranges used for vulnerability scans shall be reported to the customer upon request.

Offensity scans a maximum of one underlying IP address per subdomain.

2.2.1 Permission To Attack

The vulnerability scans ("security scans") can be "intrusive" and "non-intrusive".

- **Intrusive security scans** are scans that can circumvent the technical or organisational security measures. These scans require legally binding consent from the customer or an administrator stating that the activated subdomains under each domain (including the underlying IP addresses) can be scanned for vulnerabilities by Offensity ("Permission To Attack"). Without such a declaration of consent, these scans may be illegal.

[1] The WHOIS directory is a public list of domain names and contact data of people or organisations associated with them.

- **Non-intrusive security scans** are scans that do not circumvent any technical or organisational security measures to determine the presence of vulnerabilities. This includes, for instance, determining software versions. Generally, this does not require consent from the system owner.

For more detailed information, see Terms of Service 2.3.

2.3 "Deep web" monitoring

Involuntarily published data sets from third-party platforms can result in security problems because of email addresses and login credentials of users who use these platforms can fall into the hands of outside parties. Offensity monitors the "deep web" (also called "hidden web") to detect published data. Discovered data sets are selected and verified based on the customer domain in order to promptly inform customers of published data sets.

Offensity compares the customer's domains and IP addresses to public and partially public block and blacklists to detect a limitation in the customer services as early as possible. Entries in these lists can also indicate misuse of or compromising of customer systems.

2.4 Solution-oriented reports

The results of the ongoing scans are made available in the form of a written report via the Offensity reporting dashboard. The potentially detected vulnerabilities are categorised, the vulnerability is described and, if applicable, additional information and instructions will be provided to rectify the vulnerability. The report is drafted in English.

3 Scope of performance

Offensity includes the following deliverables:

- Offensity Security Monitoring including "2.1 Domain-based asset discovery", "2.2 Vulnerability scans and risk assessment", "2.3 'Deep web' monitoring"
- Access to the Offensity dashboard (see "2.4 Solution-oriented reports")

4 Additional services

The customer has the option of ordering additional services for Offensity for a fee. Additional services must be explicitly specified in the contract in order to be utilised.

4.1 Collaboration calls

With collaboration calls, the customer has the opportunity to utilise security consultation meetings regarding provided and future services. Unless otherwise stipulated in the contract, the duration is limited to two hours at a time, once per month.

The meeting is conducted in order to discuss identified risks and plan and coordinate potential future tests. The coordination meeting on the phone must be actively requested by the customer at least two weeks in advance. The date shall be mutually agreed upon. A1 Digital recommends agreeing on a recurring date. If the customer misses a collaboration call through its own fault, the claim for that month shall expire without replacement. If the collaboration call is not conducted for other reasons, it can be held within a month.

A1 Digital offers an encrypted communications channel for collaboration calls. If the customer wants to use a communications channel other than that recommended by A1 Digital, the customer shall bear the responsibility with respect to confidentiality of the communication. If the communications channel recommended by the customer suffers a technical malfunction, the customer shall be considered at fault. Collaboration calls are conducted exclusively via the Internet or telephone systems (mobile or landline).

4.2 Red teaming

With red teaming, A1 Digital offers a monthly pool of resources (person days) which can be used for security assessments of systems and organisations.

4.2.1 Types of assessments

The customer has the option of agreeing on the following assessments within the agreed upon framework of resources:

a) Security assessment of externally accessible systems that are continuously scanned by Offensity and/or which have been explicitly approved via a permission to attack (see **Terms of Service Section 2.3**).
b) Security assessment of the customer's internal network infrastructures after explicit approval.
c) Customised social engineering campaigns (e.g. phishing campaigns via email)

Unless otherwise mutually agreed on at least two weeks prior to the start of a monthly assessment, the service described in Item a) shall be provided. For all other assessments described in Items b) and c), a written permission to attack must be issued at least two days prior to the start of the execution of the manual assessment (see **Terms of Service Section 2.3**). Otherwise, the service described in Item a) shall be provided.

4.2.2 Internal network infrastructure

The service described in **Section 4.2.1** b) requires the installation of a "jump host" within the customer's network infrastructure. This is a virtual machine or installation file to be provided by A1 Digital. The installation and establishment of the network connectivity must be ensured by the customer. Via the jump host, A1 Digital assessors can access the network segment to be tested via the Internet. The jump host, in coordination with the customer, can also be used to perform automated tests and scans of the internal customer infrastructure prior to executing the manual assessments. If A1 Digital assessors are unable to access the jump host due to installations not being installed on time or a lack of network connectivity, the service described in **Section 4.2.1** a) shall be provided as an alternative.

4.2.3 Authenticated tests

In the framework of the collaboration calls (see **Section 4.1**), the customer has the ability to make login credentials for applications accessible to A1 Digital assessors in order to have them perform authenticated assessments.

4.2.4 Assessment period

The assessment period shall be determined by A1 Digital and coordinated with or otherwise communicated to the customer during the collaboration calls (see **Section 4.1**). A1 Digital has the right to provide monthly resources on consecutive days. If A1 Digital does not provide the agreed upon scope of resources within a month, A1 Digital can provide the days within the subsequent two months. If the postponement was caused or ordered by the customer, regardless of who is at fault, the deadline shall increase to six months. The services shall be invoiced monthly regardless of the provision of services.

4.2.5 Miscellaneous

All assessments and tests are performed via the Internet. Potentially created reports, assessments and records are then transmitted to the customer in a digital format via a channel to be specified by A1 Digital.

All assessments and tests follow a time box and grey box approach. That means the discovery of security gaps is subject to limitations due to time (time box) and resources and knowledge about internal system specifications (grey box).

The more time, resources and knowledge are available to an A1 Digital assessor, the more options the assessor has to identify security risks.

5 Data protection attachment to service description

In the framework of the services we provide, we will process your personal data as a contract processor pursuant to Art. 28 of the General Data Protection Regulation (GDPR).

1. Subject of the order

1.1. The order for the person responsible for processing to the contract processor includes the following products or services: **"Offensity"**

1.2. The following data types can be the subject of regular processing:

(Please modify based on product/service)

- ☒ Personal master data
- ☒ Personal IDs
- ☐ Special personal data
- ☒ Marketing/sales data with reference to a person
- ☒ Personal roles/associations
- ☒ Customer inventory
- ☒ Customer interactions
- ☒ Traffic data
- ☐ Movement data | Geolocation data
- ☒ Content data
- ☒ Financial data
- ☒ Login, passwords

1.3. Group of persons affected by the data processing:

(Please modify in accordance with the performance agreement)

- ☒ Customer of the client - natural person
- ☒ Customer of the client - legal entity
- ☒ User of the enterprise customer
- ☒ Employee of the client
- ☒ Contract partner of the client
- ☐ Children or persons requiring protection

2. List of commissioned subcontractors

Name	Company address	Type of processing	Processing location
Akenes SA (Exoscale)	Boulevard de Grancy 19A 1006 – Lausanne	Hosting Services	Switzerland, Germany, Austria, Bulgaria

	Switzerland		
Google Ireland Ltd. (Branch of Google LLC)	Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland	Hosting Services	Ireland, Frankfurt
Elasticsearch B.V.	Rijnsburgstraat 11, 1059 AT Amsterdam, the Netherlands	Hosting Services	Frankfurt

3. Technical organisational measures

The contract processor shall ensure security in accordance with Art. 28 (3) lit. c, (32) of the GDPR, in particular, in conjunction with Art. 5 (1), (2) of the GDPR. Overall, the measures to be implemented are measures to secure data and guarantee a level of protection commensurate to the risk with respect to the confidentiality, integrity, availability and capacity of the systems. The state-of-the-art, the implementation costs and the type, scope and purpose of the processing and the various occurrence probabilities and severity of the risk to the rights and freedoms of natural persons pursuant to Art. 32 (1) of the GDPR must be taken into account. Unless stipulated in more detail in the performance agreement, the contract processor is responsible for ensuring that a protection level appropriate for the respective processing is ensured, in particular, by means of a combination of the technical organisational measures specified below. The contract processor is permitted to implement adequate, alternative measures. The protection level of the defined measures must be reached.

A. CONFIDENTIALITY (ART. 32 (1) LIT. B OF THE GDPR)

- **Admission control:** Protection against unauthorised access to data processing systems, e.g. using magnetic or chip cards, keys, electrical door openers, factory security or gatekeeper, alarm systems, video systems.
- **Access control**: Protection against unauthorised system use e.g. (secure) passwords, two-factor authentication.
- **Login control**: No unauthorised reading, copying, modification or removal within the system, via e.g., authorisation concepts and need-based access rights, documentation of logins.
- **Separation control:** Separate processing of data collected for different purposes, e.g., by means of standard authorisation profiles on a “need to know basis”, client-capability.
- **Pseudonymisation**: If possible for the respective data processing, the primary identification properties of the personal data in the respective data processing will be removed and stored separately.
- **Classification scheme for data:** Based on statutory obligations or self-assessment (secret/confidential/internal/public).

B. DATA INTEGRITY[2] (ART. 32 (1) LIT. B OF THE GDPR)

- **Transfer control**: No unauthorised reading, copying, modification or removal during electronics transmission or transport, e.g. as a result of encryption.

- **Entry control**: Determination of whether and from whom personal data has been entered into, modified or removed from data processing systems, e.g. by means of logging.

C. AVAILABILITY AND CAPACITY (ART. 32 (1) LIT. B OF THE GDPR)

- **Availability monitoring**: Protection against random or deliberate destruction or loss, e.g. by means of a backup strategy (online/offline; on-site/off-site), uninterrupted power supply (UPS), firewall, reporting channels and contingency plans.

- **Restorability**

D. PROCEDURE FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION (ART. 32 (1) LIT. D OF THE GDPR; ART. 25 (1) OF THE GDPR)

- **Data protection management, including regular employee training**
- **Incident response management**
- **Data protection-friendly defaults**:
- **Order monitoring:** No contract-based data processing pursuant to Art. 28 of the GDPR without corresponding instructions from the client

[2] Prevention of (unintentional) destruction/deletion, (unintentional) damage, (unintentional) loss, (unintentional) modification of personal data.