A1 Digital International GmbH & Co KG Lassallestraße 9, 1020 Vienna

Offensity Security Monitoring & Reporting

Terms of service

Version: 4.0

Date: 13 Dec. 2019

Table of Contents

1. General Information 2
2. Usage prerequisites 3
2.1 Domain ownership 3
2.2 User authorisations 3
2.3 Permission To Attack 3
2.4 Technical requirements 4
3. A1 Digital International GmbH Services 4
3.1 A1 Digital service information 4
4. Service availability 4
5. Exclusion of liability 5
6. Termination, minimum contract term 6
7. Data protection and data security 6

1. General Information

The German version of these terms of service 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!

These terms of service apply starting 13 Dec. 2019. It details the use 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 stipulated here, A1 Digital's General Terms and Conditions for cloud and software solutions apply: https://www.a1.digital/at/ueber-a1-digital/agbs/.

All Offensity products 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). All offered applications comply with Offensity's service description.

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

2. Usage prerequisites

2.1 Domain ownership

In order to be able to use Offensity, the customer must either be the domain owner or obtain approval from the domain owner and legally and bindingly guarantee it is authorised to authorise the security scans.

2.2 User authorisations

To provide Offensity, we require the first and last name, email address and mobile phone number of the person(s) in whose name(s) the initial login and thus the user authorisations of an administrator are to be set up. Administrators have the following user authorisations:

- Access to all reports
- Receipt of email alerts and SMS notifications
- Activation and deactivation of additional domains and subdomains (including the underlying IP addresses)
- Issuance of a legally binding permission to attack (see "2.3 Permission To Attack")
- Creation of additional administrators

2.3 Permission To Attack

Before the "intrusive security scans" described in the service description can be executed, the customer or an administrator must issue a binding declaration of consent stating that the subdomains to be activated under every domain (including the underlying IP addresses) can be scanned for vulnerabilities by Offensity. Without such a declaration of consent, these scans may be illegal.

The customer or an administrator can add additional or delete already activated domains and subdomains via the Offensity dashboard. These automatically fall under the previously issued domain-based permission to attack.

If the permission to attack has to be expanded beyond domains for the purpose of additional testing (e.g. in the framework of the "additional services" described in Item 4 of the service description), the permission to attack can be issued in writing by an administrator. This might be needed, for example, for IP-based objectives, internal networks or the release of social engineering campaigns, for instance, as part of expanded service packages. If communicated in writing by the customer, an issued

permission to attack remains valid for a defined period of time or, alternatively, until the end of the contract term or until it is revoked.

2.4 Technical requirements

In addition, to use Offensity, the customer must meet the following requirements which are not components of the product:

- a stable Internet connection
- Internet browser (Microsoft Edge, Firefox, Chrome)

3. A1 Digital International GmbH Services

3.1 A1 Digital service information

This service includes information about the service availability and deals with all questions pertaining to invoices and data protection.

You can send an email to ask.security@a1.digital and will receive the following information:

- Service availability for your Offensity service
- Information about received invoices
- Data protection requests

Note: This service does not include any technical support services.

4. Service availability

Note: This service does not include any technical support services.

- Usage time: Monday to Friday, 09:00am - 5:00 pm.
  The usage time is the period during which the principle service is available for the customer to use.
- Observation period: one calendar year
- Offensity availability: 96%
  The availability, expressed as a percentage, is the ratio between the time during which an agreed upon service was usable in accordance with the contract and the observation period. Only critical errors are relevant to availability.

$$Verfügbarkeit\ [\%] = \frac{(Beobachtungszeitraum - nicht\ verfügbare\ Zeit)}{Beobachtungszteitraum} \times 100$$

- Maintenance window: Regular maintenance of Offensity services may require a scheduled interruption of service. Therefore, interruptions required to perform maintenance on the service will be planned by Offensity for a period of time that is defined in advance: the so-called maintenance window. In addition, special maintenance work required for operation, but outside the maintenance window can be performed by A1 Digital.
  Outside delays can result in an extension of the maintenance work for which A1 Digital is not responsible.
  The maintenance window is Wednesday from 2:00 pm to 6:00 pm.

5. Exclusion of liability

A1 Digital would like to note that the execution of security scans may limit the availability and integrity of the target systems. It is possible that proper operation may only be able to be restored by manually accessing the target system. That means, for instance, that websites on the target system may no longer be reachable or that registrations, logins or orders may be executed with incorrect data. This excludes liability on A1 Digital's part.

Every identified subdomain must be explicitly released by the customer so it can be scanned. By activating the subdomain, the customer bindingly declares it is authorised to have the underlying IP addresses attacked. When changing the DNS entries to additional or other IP addresses, the customer is obligated to deactivate the subdomain. If it is not deactivated, Offensity is allowed to assume that the customer is authorised to attack the updated IP addresses.

The customer shall conclusively resolve all questions pertaining to rights to the domains (e.g. registration, ownership, blocks, purchasing, rental, leasing, sharing, copyrights, name rights, trademarks, etc.) and other potentially resulting conflicts within its own scope of responsibility.

A1 Digital is only liable in the event of intent or gross negligence. Liability for lost profit, missed savings, loss of interest, direct and consequential damages, immaterial damages, damages from claims from third parties as well as claims for lost or modified data is excluded. The customer shall fully indemnify A1 Digital against all claims for damages asserted and suits filed by third parties based on a breach of provisions in this agreement by the customer, excluding damages that result fully from actions within A1 Digital's sphere of influence.

All technical tests and assessments do not guarantee absolute security for systems, data or processes. A1 Digital does not assume any responsibility for existing vulnerabilities being detected. Depending on the selected configurations, it is, for

instance, always possible that individual systems or vulnerabilities might be overlooked.

6. Termination, minimum contract term

There are minimum contract terms for contracts with A1 Digital for all Offensity products which you, as a customer, can select during the purchase process (monthly, annual). If the contract is not terminated by no later than 5 days prior to the expiration of the minimum contract term or extension binding period, it automatically extends by the respective periodic interval. With respect to the termination of the contract, amendments and adjustments, A1 Digital's terms apply; Specifically these are: General terms and conditions for A1 Digital cloud and software solutions.

In the event a subscription is terminated, access to the instance will be deleted.

7. Data protection and data security

The service is operated at data centres within Europe.

Further information can be found on our website: https://www.a1.digital/at/ueber-a1-digital/datenschutzerklarung/.

A1 Digital International GmbH's general terms and conditions for contract processing (AGB AVV) apply. You can find these at https://www.a1.digital/at/ueber-a1-digital/agbs/.