Antigena Email – Data Storage and Security Schedule

Summary

1. Antigena Email is an autonomous response module that takes action against email-borne attack campaigns. Hosted in one of Microsoft Azure or Amazon AWS the Antigena Email Cloud ("AEC") to provide insight and control over a Customer's email activity.

2. The AEC AI operates to extract metrics and meta data from Customer's Office365 (or equivalent cloud email system) email traffic to develop a 'pattern of life' for email activity. By correlating data across email and network traffic, AEC is able to evaluate the level of threat posed by an email and to spot unusual, anomalous emails that have bypassed existing email gateway tools.

Data Transfer and Storage

3. All data is encrypted in transit and at rest within AEC.

4. Where data is stored on the cloud, Darktrace will maintain Customer Data in the hosted location specified on the Product Order Form (unless otherwise directed by Customer). As Darktrace has no control of Customer Data uploaded to AEC, it shall remain strictly Customer's responsibility to ensure that the uploading of such data complies with international data protection laws and regulations governing the international or cross- border data transfer of information.

Data Retention and Transfer

5. Data is retained on the AEC at different rates which depend on the type of data. All data retention polices are in control of the client and can be configured via the 'Config' page. Data retention may be dynamically reduced by the instance to optimise performance. Retention categories include:

    - Log Metrics
    - Derived and aggregated data
    - Raw email data
    - Actioned email
    - Flagged email

6. A full list of extracted and derived metrics is available within the Email Console 'Advanced' tabs. No searchable facility exists over the content of emails, or attachments or links contained therein. The ability to download emails from the user interface is not available for any account not under the control of Customer's organisation. The content and body of emails is not searchable by Darktrace and does not form part of the detection function other than as a source for the extraction of these metrics and to permit the end-user recovery options. Any original email buffered and maintained in storage is individually encrypted above and beyond the instance storage encryption. At the end of the applicable retention period as set forth in the policies, raw emails will be securely erased.

7. Customer's AEC will provide information to detect and respond to anomalous email activity. AEC will supply information to enable Customers to respond to email borne threats.

8. The telemetry data that is in the AEC is limited to the following:

    - Probabilistic data structures which describe the pattern of activity, Darktrace rarity and frequency scores of visited hosts, domains, file hashes and links seen in the Darktrace monitored environment. These data structures do not include any of these details in an extractable format
    - Hostname, IP, MAC address, Operating system, Device label and time of last seen are transferred
    - Darktrace Alert information. Notifications of Alerts occurring as a result of anomalous network activity may be transferred to the AEC instance for the purposes of security forensics.
    - A mapping between those properties and nominated AEC models
    - Email addresses, naming, and groups found in emails and any associated email repositories

Data Access by Darktrace

9. Access to AEC by Darktrace personnel is limited to the following purposes:

    - Initial set up, configuration and traffic validation
    - Access for the creation of customer reports (as part of trial, or as an on-going service agreement)
    - Security incidents
    - Support incidents

10. All email data access is logged and controlled. Logs of all data access, whether made by Customer or by Darktrace personnel, is available to Customer through the audit page in the interface. The body content of original emails is not available to Darktrace personnel through the interface and emails are individually encrypted.

11. There is no part of the workflow of any Darktrace personnel that requires access to original email.

12. Elements of emails, which already have a degree of anomaly associated with them, including attachment details and links and their derived properties may be collated by the Darktrace SOC (Security Operations Centre) for the purposes of analysis and security enhancement.

Link Operations

13. Under certain circumstance, and as dictated by Darktrace or Customer models, links present in emails may be rewritten to redirect any user clicking that link via a Darktrace service. This link service will download the content of the destination of the original link and apply additional security checks on that destination and its content. Darktrace reserve the right to utilise third party services for elements of this security checking. No part of the service will identify to those third parties any details of the user, or organisation, performing the click action. Darktrace models will only re-write a link if some level of anomaly is detected that gives a reasonable suspicion that additional security checks may be necessary.

Data Protection

14. Darktrace will protect any Customer Personal Data processed by AEC in accordance with the Data Protection Addendum at Appendix 2 of the Master Customer Agreement, and additionally subject to the following:

    a. Details of Processing:

        i. Subject Matter: Customer email traffic

        ii. Duration: As set forth in the Product Order Form or as specified by system configuration

        iii. Purpose: The provision of AEC

        iv. Nature: Storage, compute and analysis of Customer email traffic

        v. Type of Personal Data: Customer Data uploaded to AEC

        vi. Categories of Data Subjects: May include Customer's customers, employees, suppliers and end-users

    b. Sub-processors:

        i. Customer hereby authorises Darktrace to use Amazon AWS or Microsoft Azure as applicable (the "Cloud Provider") as a sub-processor to fulfil its contractual obligations under the Agreement. Customer acknowledges that this authorisation will extend to and include the sub-processors used by the Cloud Provider, a list of which is available at the Cloud Provider's website.

        ii. Darktrace will have in place with the Cloud Provider a written agreement equivalent to the terms contained herein to protect Personal Data.

        iii. The Cloud Provider will ensure the security of any Personal Data processed by reason of this Agreement in accordance with its standard security measures and practices.

        iv. Darktrace will remain responsible for all acts or omissions of the Cloud Vendor under this Agreement.

    c. Transfers of Personal Data:

        i. Customer will specify the location where Customer Data will be hosted (the "Region"). Once selected, neither Darktrace nor the Cloud Provider will transfer Customer Data from the Region except as necessary to provide the AEC offering or to comply law.

        ii. The EU Model Clauses shall apply to the extent the processing of Personal Data by the Cloud Provider involves a transfer of Personal Data which originates in the EEA to a third country outside of the EEA. For such purposes, Customer hereby authorises Darktrace to enter into the EU Model Clauses with the Cloud Provider on Customer's behalf.