Appendix 3 – Technical Requirements Policy

Service Partner Requirements v1.1 May 2023

Introduction

Darktrace considers the security and privacy of its customers' data as its primary purpose and reason for existing. We take great care to design systems and processes that protect this data from:

- Hostile outsiders
- Other customers
- Insider threat
- Accidental mishap

As a Darktrace partner providing services to our customers we require you to meet certain minimum requirements in this spirit.

Standards

Service partners are expected to show their dedication to security by meeting well known international standards such as:

- ISO27001 and associated standards
- AICPA SOC 2 Type II
- CSA STAR
- NIST 800-171 / CMMC Level 3

(standards not in the list above may be acceptable, please ask your account manager)

Specific Controls

The partner will have a documented security policy that includes the following minimum controls:

Encryption

1. All customer data will always be encrypted at rest with AES 256 or better ciphers. This includes on the infrastructure and on any staff devices.
2. All customer data will always be encrypted in transit with ciphers from the current Intermediate or Modern list at:
   - https://wiki.mozilla.org/Security/Server_Side_TLS.
   - https://infosec.mozilla.org/guidelines/openssh
3. Older ciphers must not be offered during protocol negotiation.

Maintenance

4. All staff equipment and service infrastructure will use operating systems that are still supported for security updates.
5. All staff equipment and service infrastructure will be patched with the latest security updates within 30 days of their release.

Authentication

6. All remotely accessible logins for any service and its supporting infrastructure for both users and admins will be protected with multi-factor authentication that is not reliant on the security of the underlying communications system. To elaborate, 2FA codes must not be sent by unencrypted SMS, email or phone call [1].

7. The partner will implement an access control system based on least-privilege to restrict access to both customer data and the controlling infrastructure in both physical and digital realms.

Monitoring

8. The infrastructure and devices used for performing the service must be monitored by a Darktrace Enterprise Immune System with high priority breach alerts feeding to a Security Operations team capable of responding 24/7/365.
9. Any compromises of this infrastructure or customer data must be reported to Darktrace security within 24 hours of their detection. Details of the breach must not be sent in an open email.

Multi-tenancy

10. Where call home is provided, each customer's endpoint must be sufficiently isolated from others such that Darktrace products cannot inadvertently or through deliberate outsider manipulation communicate with the incorrect customer environment. Each customer must be run in a separate virtual machine/container or similar.

Staff

11. Any staff with access to Darktrace customer data will be vetted including the following checks (where available in local jurisdictions):

    a. Identity verified
    b. References and education verified
    c. Criminal Records check
    d. Credit check

12. All staff will receive regular Security Awareness training

Works Cited

[1] Microsoft, "It's Time to Hang Up on Phone Transports for Authentication," 10 November 2020. [Online]. Available: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/it-s-time-to-hang-up-on-phone-transports-for-authentication/ba-p/1751752.