Professional Service Days

This Service Definition is subject to the Darktrace Master Services Agreement (as found at https://www.darktrace.com/legal/master-services-agreement) and applicable Product Order Form.

1. High Level Summary

Professional Services (PS) Days provide Customers with flexible access to Darktrace's expert resources to support deployment, configuration, optimization, and integration of Darktrace products. These days are designed to support with value realization, complex use cases, and adoption of Darktrace's Cyber AI capabilities. PS Days can be delivered either remotely or on site depending on customer preference and Darktrace's availability.

2. Expected delivery

2.1 Scope

Professional Services Days are designed to provide flexible, expert-led support across a wide range of activities tailored to the Customer's deployment's maturity, strategic goals, and operational needs. These days are scoped collaboratively and delivered by Darktrace's Professional Services team, which may include Cyber Infrastructure Engineers, Cyber Solution Architects, Project Managers, and Customer Success Managers.

Professional Services Days may be used for a range of activities, including but not limited to:

- **Deployment & Configuration**
  - Assistance with initial or expanded deployment of Darktrace products.
  - Configuration of sensors, connectors, and integrations.
  - Validation of data ingestion and model training.
- **Use case activation and tuning**
  - Identification and implementation of relevant use cases.
  - Tuning of detection logic and response workflows.
  - Mapping of use cases to business priorities or compliance frameworks.
- **Integration with upstream/downstream systems**
  - Technical guidance on integrating Darktrace with SIEM, SOAR, cloud platforms, ticketing systems, and other third-party tools.
  - API configuration and automation setup.
  - Validation of data flows and alerting mechanisms.
- **Health & Optimization sessions**
  - Review of deployment health and performance.
  - Recommendations for tuning, scaling, or re-architecting.
  - Identification of gaps or inefficiencies in current usage.
- **Strategic advisory and roadmap planning**
  - Strategic advisory sessions on roadmap planning.
  - Maturity modeling.

2.2 Booking Process

PS Days must be scheduled in advance through a Customer Portal ticket entitled 'Professional Services Days request'. For on-site PS days, ticket requests must be raised at least 3 weeks in advance of the proposed date the site visit. For remotely delivered PS days, ticket requests must be raised at least 2 weeks in advance of the proposed remote session. Unless otherwise agreed, a minimum of 1 full PS Day per booking is required. Multi-day engagements may be delivered consecutively or spread across weeks depending on availability and scope. Deliverables (e.g., reports, configurations, recommendations) will be documented and shared post-engagement. Darktrace will make commercially reasonable efforts to align resources with customer priorities and timelines.

PS Days are subject to geographic eligibility. Darktrace can only provide on-site services in locations situated within countries that have been approved by Darktrace. Prior to scheduling a PS Day, Customer must ensure that the on-site service location is within an approved country. Darktrace reserves the right to decline or reschedule any on-site service request for locations outside the approved countries list.

2.3 On-site Delivery Process

When Professional Services Days are delivered onsite, the following process and expectations apply.

2.3.1 Pre-Visit Planning

On-site visits must be scheduled for at least 3 weeks in advance, subject to resource availability and travel logistics. A detailed plan for each day must be agreed upon prior to the visit, including objectives, expected outcomes, and required access. Darktrace reserves the right to reschedule or decline sessions if planning requirements are not met.

Darktrace will coordinate travel and lodging arrangements in accordance with the customer's visitor policies and Darktrace's travel guidelines.

2.3.2 Customer Site Requirements

Appropriate authorized Customer representatives must be present and accompanying Darktrace personnel at all times

When attending a Customer site, the following must be provided to applicable Darktrace personnel:

- A secure workspace with internet access and power outlets;
- Temporary credentials or guest access to relevant systems; and
- Escort or badge access if required by site security policies.

2.4 Remote Delivery Process

When Professional Services Days are delivered remotely, the following process and expectations apply.

2.4.1 Pre-Session Planning

Remotely delivered PS days must be scheduled for at least 2 weeks in advance, subject to resource availability. A detailed plan for each day must be agreed upon prior to the session, including objectives, expected outcomes, and required access. Darktrace reserves the right to reschedule or decline sessions if planning requirements are not met.

2.4.2 Customer Requirements

- Remote PS Days should run on Customer's collaboration technology, such as Microsoft Teams or Zoom
- Customer must coordinate and ensure attendance of relevant stakeholders needed to fulfil the plan agreed upon
- Customer must take detailed notes and will be solely responsible for documenting action items as appropriate, during the session

2.5 Daily Structure

Unless otherwise agreed in writing, a typical PS Day runs from 9am to 5pm local time, with limited flexibility for out of hours support, subject to availability. The PS Day will start with a kick-off meeting to set the agenda for the day and align on goals and logistics. The contents of the PS Day will be determined by the agreed upon activities in the pre-visit planning. A wrap-up session will be held at the end of each PS Day to review progress and plan next steps.

2.6 Post-Session Follow-Up

Following a PS Day, Darktrace will provide a summary of activities, findings, and recommendations within 5 business days of the session. Any deliverables or configurations will be documented and shared securely, typically via the Darktrace Customer Portal. Follow-up sessions may be scheduled to continue work or address outstanding issues in accordance with the number of allotted PS Days in the POF, and relevant services otherwise included in the Offering.

3. Requirements

Prior to the use of PS Days, the following must be in place:

- A valid Darktrace subscription and active deployment;
- Completion of initial onboarding (if applicable);
- Agreement on scope and objectives for each PS Day (pre-visit planning); and
- Customer must be current on fee payments at the time of scheduling.

Set out below are the access technical requirements in each coverage area:

1. /NETWORK:

   - Customer must have access to managed switches that can support port mirroring. Alternatively, Customers can utilize network TAP/Packet Brokers to send traffic to Darktrace for analysis.
   - Customer must have access to Firewalls to make necessary rules for communication.
   - In scenarios where virtual sensors like vSensors are required, Customer needs access to Darktrace Customer Portal to download the sensors and access to their virtualized environments to install the sensors.

2. /EMAIL:

   - Customer must have access to a global or super admin account for their email tenant.
   - Customer must have access to Firewall to make necessary rules to allow communication with the Darktrace/Email instance.
   - Darktrace/Email is only available to organizations with specific licenses due to Google Workspace restrictions on Third-Party Email Archiving: Google Workspace Enterprise or Enterprise for Education License (or above). Consult the relevant Product Guide on the Darktrace Customer Portal for other licensing restrictions

   /EMAIL – DMARC:

   - Darktrace / EMAIL - DMARC is available exclusively for Microsoft 365 / Office 365 Customers. Google Workspace and other email providers are not supported.

   /EMAIL Data Loss Prevention:

   - Access to the Microsoft Exchange Admin Centre to complete the configuration process.
   - Access to the Config page of the Darktrace ⁄ EMAIL Console to gather relevant information during configuration.
   - A valid SMTP host (ending in protection.outlook.com) for all enabled domains.

  - An email address external to the organization which is suitable for a simple test procedure during configuration.

3. /IDENTITY:

- Customer must have Administrator permissions to authorize each Darktrace/IDENTITY module.
- Please consult the relevant Product Guide on the Darktrace Customer Portal for App-specific requirements or licenses.

4. /ENDPOINT:

- If Call Home is available, a Darktrace deployment running a minimum of Darktrace Threat Visualizer 5.2 is required. If Call Home is not available, the associated deployment must be running Darktrace Threat Visualizer 6.1 or above.
- Customer must have access to all endpoints where cSensors should be installed.
- Customer must have access to firewalls to make necessary rules to allow communication between the sensors and the rest of the Darktrace deployment.

5. /OT:

- Customer must have access to managed switches that can support port mirroring. Alternatively, Customers can use network TAP/Packet Broker to send traffic to Darktrace for analysis.
- Customers must have access to Firewalls to make necessary rules for communication.
- For air gapped networks, Customer must have access to those networks to be able to install Darktrace products.

6. /CLOUD:

- Customer must have access to an account on the Cloud Service Provider, with permissions required to make necessary changes.
- Customer must have permission to create CloudTrails, Cloudformation Stacks, and StackSets in the management account and child accounts.

7. /Proactive Exposure Management:

- A configured Darktrace environment with Darktrace /Network running the most recent Threat Visualizer software.
- A configured Darktrace/Email for Microsoft 365 and Google Workspace deployment.
- Permitted outbound connectivity from the Darktrace instance to required endpoints.

8. /Attack Surface Management:

- A Darktrace Threat Visualizer instance running the most recent software version (minimum 5.2).
- An API key for authentication with your Darktrace PREVENT/ASM environment. This can be requested from Darktrace support if not possessed already.

9. /Incident Readiness & Recovery:

    - A Darktrace Threat Visualizer instance running the most recent software version (minimum 6.1).
    - A Darktrace ⁄ Incident Readiness and Recovery license key

10. /Forensic Acquisition & Investigation:

    - AWS:
        - The deployment can be executed using Terraform or AWS CloudFormation. Multi-account deployments will require a cross-account role to be deployed in all accounts intended for FAI acquisitions. The cross-account role can be created using CloudFormation StackSet or through Terraform
        - The user who is running the installation will need access to the following services:
            - EC2 (for instance, VPC, and optionally Load Balancer creation)
            - IAM (for role and policy creation)
            - CloudFormation (if used for deployment)
        - Typically, a user with Admin permissions is recommended.
    - Azure:
        - The deployment can be executed using Terraform. Multi-subscription deployments will require an Application Registration to be created.
        - The user who is running the installation will need access to the following services:
            - Compute (for VM and VNet creation)
            - RBAC Role Assignments
            - Application Registration in Entra ID
        - Typically, a user with Owner privilege to Azure and Global Admin to Entra ID is recommended
    - GCP:
        - The deployment can be executed using Terraform. For multi-project deployments, manual adjustment of Service Account permission scopes is required.
        - The user who is running the installation will need access to the following services:
            - Compute (for VM and VPC creation)
            - IAM (for Service Account creation)
        - Typically, a user with Owner privilege is recommended

4. Customer Responsibilities

Customers are advised that Darktrace may only offer advice on Darktrace products, and to check their Darktrace coverage areas before requesting assistance. It is Customer’s sole responsibility to apply and maintain any recommendations offered by the Darktrace engineer as part of the Service, and Customer accepts that, if the recommendations are not followed, it may result in an associated reduced level of the Darktrace Offering.

The Customer is solely responsible for ensuring the success of Professional Services Days by fulfilling the following best practices:

Resource Coordination

- Assign a dedicated person to oversee engagement logistics and act as the primary point of contact.
- Ensure availability of relevant stakeholders (e.g., Security, IT, Networking, Legal, Compliance) during scheduled sessions.

Access & Infrastructure

- Provide timely access to systems, environments, and data sources required for service delivery.
- Ensure that necessary infrastructure (e.g., sensors, connectors, APIs) is operational and accessible.
- Facilitate on-site access for Darktrace personnel as needed.

Preparation & Planning

- Define clear objectives and desired outcomes for each PS Day in collaboration with Darktrace.
- Share relevant documentation, network diagrams, and architectural overviews in advance.
- Notify Darktrace of any planned changes to infrastructure or security policies that may impact service delivery.

Engagement Support

- Participate actively in workshops, working sessions, and reviews.
- Provide feedback on deliverables, recommendations, and findings.
- Coordinate internal testing and validation of configurations or integrations.

Security & Compliance

- Ensure that all shared data complies with applicable privacy, security, and regulatory requirements.
- Inform Darktrace of any data handling restrictions or compliance obligations that may affect service scope.

Change Management

- Communicate any changes to scope, priorities, or timelines in a timely manner.
- Manage internal approvals and change control processes related to service activities.

Health & Safety

- Any required safety briefings or documentation must be provided in advance.

Post-Engagement Follow-Up

- Review and sign off on completed work or deliverables.
- Implement agreed-upon recommendations or configurations.
- Maintain continuity of internal ownership for ongoing initiatives.

5. Considerations

The following considerations should be reviewed and acknowledged prior to the use of Professional Services Days:

- Dependency on Deployment Maturity

  - The effectiveness of PS Days is contingent on the maturity and stability of the customer’s Darktrace deployment. Incomplete or unstable environments may limit the scope or impact of services delivered.

- Infrastructure & Data Availability
  - Many activities (e.g., forensic investigations, integration work) rely on timely access to logs, network traffic, endpoint data, and third-party systems. Delays or restrictions in access may impact delivery timelines or outcomes.

- Third-Party Coordination
  - Where integrations or data flows involve third-party vendors (e.g., SIEM, SOAR, cloud platforms), customer coordination with those vendors is essential. Darktrace cannot guarantee outcomes where third-party cooperation is limited or unavailable, nor will Darktrace coordinate directly with third-party vendors, service providers or contractors engaged by Customer.

- Third-Party IT Technologies
  - Darktrace personnel will not access, configure or otherwise utilize any third-party security or network technologies (including but not limited to switches, firewalls, routers or similar systems) used by the Customer. Darktrace will further not coordinate, communicate or otherwise engage directly with any third-party vendors, service providers or contractors engaged by Customer. Any adjustments or changes recommended by the Darktrace representative must be implemented solely at the Customer’s discretion and sole liability.

- Licensing & Feature Access
  - Certain services may require specific product licenses or modules (e.g., Autonomous Response, /IDENTITY, IR&R workflows). PS Days do not include license provisioning or feature enablement.

- Scope Flexibility
  - While PS Days are designed to be flexible, they are not intended to replace formal project management, custom development, or long-term managed services. Activities must be scoped and agreed upon in advance.

- Security & Compliance Constraints
  - Darktrace will operate within the customer’s defined security and compliance boundaries. Any restrictions on data handling, remote access, or tool usage must be communicated prior to engagement.

- Time Allocation
  - PS Days must be consumed in full-day increments. Preparation, documentation, and follow-up activities may count toward day consumption.

- Customer Readiness
  - The success of PS Days is dependent on customer readiness, including resource availability, internal alignment, and timely decision-making. Darktrace is not responsible for delays caused by internal bottlenecks.
- No Guarantee
  - While Darktrace will make commercially reasonable efforts to deliver value during PS Days, specific outcomes (e.g., successful integration, threat detection, automation) are not guaranteed and depend on multiple external factors.

6. Roles and Responsibilities

Roles	**Responsibilities**
Customer Roles	
Customer Portal Primary User	• Uses product functionality • Serves as point of contact and escalation • Owns administration and customization of Darktrace products in their environment
Customer Portal Users	• Have access to internal systems to perform required installation steps. • Perform regular checks of Darktrace data ingestion. • Respond accordingly to Sys Status alerts to ensure optimal traffic quality and delivery. • Maintain call-home connectivity with Darktrace for the duration of installation activity.
Darktrace Roles	
Cyber Infrastructure Engineer	• Timely response to all Customers' requests. • Following Customer request, collation, and timely delivery of products in response to Customer raised requests. • Travels onsite as outlined in contract • Respond to feedback and/or requests for further assistance via Customer Portal Tickets.
Regional Professional Services Manager	• Owner of Quality Assurance process. • Ensures appropriate resources are available to provide coverage for the Service.
Escalation Point	• If Customer is not satisfied with the performance of the Cyber Infrastructure Engineer (in accordance with this Service Definition), Customer may seek escalation to the following positions as appropriate. ○ Customer Success Manager. ○ Director of Professional Services. • Receives Customer issues and uses all reasonable endeavors to resolve the escalated issues. • Provides regular updates on escalated issues until resolution is reached.

7. Assumptions

Darktrace will not be liable to provide services for any request(s) based upon:

- improper use, site preparation, or site or environmental conditions or other non-compliance with applicable Documentation or these terms;
- failure or functional limitations of any non-Darktrace software or product impacting systems receiving Darktrace Hardware Support Services;
- malware (e.g. virus, worm, etc.) introduced by Customer;
- modifications or improper system maintenance or calibration not performed by Darktrace or authorized in writing by Darktrace;
- fire damage, water damage, accident, electrical disturbances, transportation by Customer, or other causes beyond Darktrace's control;
- use not in line with a proper manner or in conditions which adequately protect and preserve the Hardware; and
- modifications made to third party software, with any such modifications made by Darktrace personnel to be made at the Customer's own instruction and risk.

NO ADVICE, ALERT, OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY CUSTOMER FROM DARKTRACE OR THROUGH OR FROM THE SUPPORT SERVICES DESCRIBED HEREIN SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED HEREIN OR IN THE MASTER SERVICES AGREEMENT. DARKTRACE SHALL NOT BE LIABLE FOR ANY ERRORS OR DELAYS IN THE CONTENT OR ALERTS AVAILABLE THROUGH SUPPORT SERVICES, OR FOR ANY ACTIONS TAKEN IN RELIANCE THEREON. THE CUSTOMER UNDERSTANDS AND ACKNOWLEDGES THAT NOT ALL ANOMALIES, INTRUSIONS, INEEFICIENCIES OR GAPS IN COVERAGE MAY BE REPORTED. ANY RECOMMENDATION ACTED UPON BY CUSTOMER IS DONE SO AT CUSTOMER'S OWN RISK AND LIABILITY.

By using this service, Customer acknowledges that Darktrace's ability to perform services envisioned by this Service Definition depends upon Customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Darktrace. Where this Service Description requires agreement, approval, acceptance, consent, or similar action by either party, such action will not be unreasonably delayed or withheld. The Customer agrees that to the extent its failure to meet its responsibilities results in a failure or delay by Darktrace in performing its obligations under this Service Description, Darktrace will not be liable for such failure or delay.