Service Description: Managed Detection and Response Service Bundle

1 Managed Detection and Response Service Bundle Composition

The Managed Detection and Response Service Bundle consists of the following Services:

- Darktrace Security Operations Support;
- Service Ready Workshop;
- Managed Detection and Response; and
- Analyst Services.

2 Darktrace Security Operations Support

Details on the Darktrace Security Operations Support Service may be found in the Darktrace Security Operations Support Service Definition found at: https://darktrace.com/legal/product-specifications-and-service-definitions.

3 Service Ready Workshop

Service Ready Check is initially required before the Managed Detection and Response Service becomes fully operational. A Darktrace Engineer will review Customer's environment at point in time via the Service Ready Check and analyze the optimization of the Darktrace deployment. For new Darktrace customers, reasonable installation and configuration work will need to have taken place before the Service Ready Check to ensure that both the Real-Time Detection and Autonomouse Response functions of Darktrace / NETWORK are in a basic operational state (see section 3.1 below). Based on findings from the Service Ready Check, a Workshop can be scheduled.

Subject to available resources, Darktrace will assign an available engineer for the time slot booked by Customers for the Service Ready Workshop. The time slot must be agreed at least 10 working days in advance. Should Customers cancel or move a Service Ready Workshop within 10 working days of the originally scheduled time slot, any rearranged time slot is subject to the same advance notice provisions. Ahead of the Service Ready Workshop, a Darktrace Engineer will conduct a Service Ready Check, the results of which will form the basis of the Service Ready Workshop.

The Workshop itself will consist of an interactive video call, wherein the Engineer will take the Customer attendees through any observations made as a result of the Service Ready review. The Engineer will make recommendations that the Customer can perform to improve the configuration of the deployment in order to help optimize performance and improve factors such as reachability, tracking and how the products act on the Customer network. Workshops are envisioned to be around one hour with one Workshop being sufficient for most deployments. In the exceptional case that additional Workshops are required, Customers are limited to a maximum of three workshops over a period of 30 (thirty) days from the initial wokshop (the Service Ready Period). No Service Ready Workshops are offered outside of the Service Ready Period.

Any review and subsequent recommendations are made on a point in time basis, that is wholly dependent on the Customer Data that the Darktrace instance has access to at the time of the Service Ready Check. Any changes made by Customer based upon recommendations provided as a part of the Service Ready Workshop are made at their own discretion. Customer acknowledges that changes made to the Customer environment after the Service Ready Workshop may impact the accuracy of any recommendations made therein.

3.1 Service Ready Check

The Service Ready Check consists of:

1. Verifying that the Darktrace Offering is initially deployed (at least one master instance is active).

2. Checking for critical and high System Status Alerts for active masters.

3. Verifying if the Autonomous Response element of Darktrace / NETWORK is fully deployed. Including:

- Checking the proportion of devices and servers are tagged for Autonomous Response Actions;
- Checking when reachability tests were last performed for the network;
- Checking if autonomous mode is active; and

- Checking for any Autonomous Response misconfigurations.

4. Verifying if the Autonomous Response element of Darktrace / CLOUD and IDENTITIES are fully deployed, if purchased. Including:

- Checking if modules are licensed and authorized; and
- Checking if autonomous mode is active.

3.2 Workshop Composition

The focus of the Workshops is intended to be centered on the results of the Service Ready Check, and addressing any issues that are highlighted therein. This includes Real-Time Dection critical & high system status alerts, Autonomous Response workflows, configuration, and testing. Any questions or analysis on integrations are to be handled separately by Customer's account team outside of the Workshop.

First, the Darktrace engineer will walk through critical issues found with Real-Time Dection operationality such as, but not limited to: disconnected appliances, low traffic, unidirectional traffic, or sub-optimal device tracking. To ensure efficacy of the Workshop, Customer should ensure that there at least one active member of its Network team is in attendance. The Network team member should have the necessary network access to make the changes needed to resolve critical alerts.

Second, the Darktrace Engineer will walk through critical issues with Autonomous Response, such as but not limited to: low tagging, running human confirmation mode, poor reachability or licensing issues. To ensure efficacy of the Workshop, Customer should ensure that there at least one active member of its Security team and/or user of Darktrace is in attendance. The Security team/User(s) should have permission from the Customer organization to update the Autonomous Response configuration as recommended in the Workshop Results below.

There is no limit to the number of Customer participants that may join the Workshop and the Customer is advised that Workshops cannot be recorded.

Lastly, once all recommendations from both the Real-Time Dection and Autonomous Response elements are shared with the Customer, the Darktrace Engineer will sign off that the Service Ready Workshop is complete, and, if applicable, that the full operationality of the Managed Detection and Response Service may be accessed.

It is the customer's responsibility to apply the recommendations offered by the Darktrace engineer. Customer acknowledges that the results of the Service Ready Check indicate the effectiveness of the Managed Detection and Response service, and accepts that, if the recommendations resulting from the Service Ready Workshop are not followed, it may result in an associated reduced level of service.

Notes of the contents of the call will be taken throughout and a summary of what was covered will be shared with the Customer after the Workshop via a Customer Portal ticket along with any relevant materials that were presented during the Workshop.

3.3 Service Ready Recommendations

The Service Ready Check and Workshop will indicate the scope of coverage of the Offering, which in turn determines the scope of the Managed Detection and Response Service. To improve the network coverage of Offering, the recommended conditions for full coverage normally include:

- NETWORK:
  - Access (Call Home) to all Darktrace master instances.
  - All issues identified within System Status resolved.
  - All devices tagged for Autonomous Response.
  - Running autonomous mode 24/7.
  - Full reachability within the network, tested through the product.
  - No poor model customizations.
- IDENTITIES:
  - Working License Key.
  - Running Autonomous Mode 24/7.

    - All Autonomous Response Modules running without errors and are authorized for actions.
- ENDPOINT:
    - Working License Key.
    - All devices tagged for Autonomous Response.
    - Running Autonomous Mode 24/7.
    - Endpoint Actions set to TRUE and a policy is set in cSensor Admin.

Should full coverage not be possible in a given environment, minimum requirements for successful operation of the Managed Detection and Response Service are included under section 4.2.

3.4 Post Service Ready Workshop

After a Service Ready Workshop, a Darktrace engineer will submit an associated report in a Customer Portal ticket that outlines the current status of Customer's Darktrace Offering. Customer may schedule up to two additional Service Ready Workshops within the Service Ready Period in the event that there are unaddressed issues after the initial Service Ready Workshop.

Once the Service Ready Period has elapsed, Customer assumes responsibility for the health of their Darktrace Offering and remediation of implementation issues, as identified by the Service Ready report, or otherwise. Customer acknowledges and accepts that unresolved issues may result in an associated reduction in scope of the Managed Detection and Response Service.

4 Managed Detection and Response Service

4.1 Service Features

The Managed Detection and Response Service monitors a Customer's NETWORK environment for significant anomalies, indicative of in-flight attack. Darktrace SOC conducts investigations of these high priority detections and alerts customers to potentially severe incidents. In addition to this, the Managed Detection and Response service also includes a review of Autonomous Response actions related to the incident, where Darktrace SOC analysts can extend Autonomous Response actions to provide additional security whilst a customer security team completes their remediation process.

Managed Detection and Response is an English language only service delivered by Darktrace's global SOC 24/7 using a follow-the-sun shift pattern.

4.1.1 Enhanced Monitoring

Darktrace SOC will alert Customer's named SOC contacts when a significant and likely high-impact Alert anomaly is detected by the Software (utilizing a subset of Darktrace's standard models identified by the label "Enhanced Monitoring").

An Enhanced Monitoring (EM) model breach will be generated when the conditions within a model tagged as 'Enhanced Monitoring' are met. As a compromised device may generate multiple Enhanced Monitoring model breaches within a short time period, to avoid duplication the number of alerts sent to Darktrace SOC is rate limited as only a single alert is required to initiate a Darktrace SOC investigation.

Darktrace SOC works closely with our model development specialists to continually review and revise the Enhanced Monitoring models used for the Managed Detection and Response service to ensure optimum detection capabilities. Models that have the 'Enhanced Monitoring' tag are only editable by Darktrace, but can be used as a template by customers, for their own alerting purposes, but will not be covered by the Managed Detection and Response Service so the 'Enhanced Monitoring' tag will be removed. Darktrace may make bespoke changes to an individual customer's 'Enhanced Monitoring' models to improve model proficiency for the customer's Managed Detection and Response service.

Once a notification of an Enhanced Monitoring model breach has been received by the Darktrace SOC team, it will be assigned to a SOC analyst. The SOC analyst will access the Customer deployment and using the Enhanced

Monitoring model breach as a start point, will investigate the activity that has been identified by Customer's Real-Time Detection service as being potentially related to an in-flight attack. The SOC Analyst will assess whether the activity should be alerted to the Customer SOC contacts or whether the activity is not significant enough to issue an alert.

4.1.2 Autonomous Response Review

In addition to the investigation, for the device(s) investigated, Darktrace SOC will also determine the status of Autonomous Response actions, which are actively being made when Autonomous Response is in autonomous mode or being suggested when Autonomous Response is in Human Confirmation mode.

Following Autonomous Response review, if the device investigated meets the criteria outlined in the Requirements section below, Darktrace SOC may perform one of the following actions:

- EXTEND any active actions suggested by associated Autonomous Response models for a period of 24hrs;
- If Autonomous Response is configured to operate in Human Confirmation mode, provide information around any pending Autonomous Response actions suggested by the model, and ACTIVDarktrace Security Operations Support any Autonomous Response actions upon written confirmation from the customer security team; or
- ACTIVDarktrace Security Operations Support a Pattern of Life (POL) action for a period of 24hrs to provide additional protection. This will prevent the device from conducting activity outside of behaviors that have been modelled by Darktrace as being usual for that device.

The following links document all current Autonomous Response actions (inhibitors):

https://customerportal.darktrace.com/product-guides/main/antigena-network-model-actions

https://customerportal.darktrace.com/product-guides/main/antigena-saas-inhibitors

Should a device, believed to be compromised, not meet the criteria outlined in the Requirements section below, Darktrace SOC will include a recommendation in the Managed Detection and Response alert sent to the customer's named contacts with the option to approve Darktrace SOC to carry out the suggested recommendations.

4.1.3 Alert Details

In the event an anomaly triggers the Enhanced Monitoring parameters and is deemed sufficiently high-risk, Managed Detection and Response alerts are delivered to customer's named contacts via an email attachment secured by a password. A Managed Detection and Response ticket with alert content will also be generated on the Customer Portal and made visible to the customer. Customer's named operators can also choose to receive an automated phone call and/or SMS message to notify them of a new alert.

4.1.4 Post-Alert Support

Although Darktrace SOC analysts may include suggested actions within a Managed Detection and Response alert, the customer maintains responsibility for all follow-up analysis and any remediation activity required, as designated by their own security/IT policies. Customers can provide feedback for Managed Detection and Response alerts using the associated Managed Detection and Response ticket generated on the Customer Portal.

In the event that a Managed Detection and Response alert is confirmed as an in-flight attack, Darktrace SOC may assist with further analysis of an investigation generated by a Managed Detection and Response alert. This is limited to a maximum of 2hrs per customer per month. Customers are encouraged to reach out to Darktrace SOC using the Managed Detection and Response ticket generated on the Customer Portal to request further assistance.

Alternatively, Customers can call the Darktrace Customer Support helpline to request a call-back from Darktrace SOC. Customers are advised that the Darktrace helpline follows strict verification protocols to protect ourselves and our customers from potentially fraudulent communications. Callers must have an active and verified Darktrace Customer Portal account and will be authenticated by providing a 2FA code or answering security questions.

4.1.5 Resolved Investigations

Should a Darktrace Analyst conclude their Managed Detection and Response investigation and determine that the anomaly identified does not indicate significant and/or high-impact activity, Darktrace SOC may choose not to alert a customer to the activity. In all cases, Darktrace SOC will add a comment on the Darktrace UI to the EM model investigated. This will include an indication of whether an alert has been raised. These comments allow customers to identify the EM models that have been investigated by the Managed Detection and Response service.

A summary of all investigations carried out on behalf of a customer is outlined in a monthly SOC report, which is made available to Managed Detection and Response customers in the Customer Portal.

4.2 Requirements

Managed Detection and Response is only available to customers using Darktrace / NETWORK or Darktrace / IDENTITIES (previously known as Darktrace DETECT/Apps and Darktrace RESPOND/Apps). If configured within / NETWORK, Managed Detection and Response can also provide coverage of / OT, / IDENTITIES and / Endpoint.

Managed Detection and Response service delivery is dependent on customers maintaining an active call-home connection with Darktrace 24/7. This connection enables notifications to be received by Darktrace SOC that an Enhanced Monitoring breach has occurred.

A Darktrace instance operating Call-home will attempt to establish a secure channel with the Darktrace infrastructure. Each Darktrace installation will have a unique hostname pre-set in the configuration, resolving to a single Darktrace central IP address. To enable Call-home to function, Darktrace must be permitted to contact Darktrace IP addresses over HTTPS/443 with SSL wrapping.

Call-home connectivity for cloud hosted deployments is mandatory and is configured by Darktrace at the time the cloud instance is established.

‘Enhanced Monitoring’ and Autonomous Response models are kept up to date automatically by enabling “Auto Update Models” in the Model Updates section on the sysconfig page of the / NETWORK UI.

Darktrace SOC will only be able to influence Autonomous Response actions on deployments running in autonomous mode, on devices that meet the following criteria:

1. Are included in the Darktrace Real-Time Dection scope of coverage;
2. Are configured to receive Autonomous Response coverage;
3. Have an active tag for Autonomous Response actions (e.g.; ‘Antigena All’, ‘Antigena External Threat’ etc.) ; and
4. Is reachable by Autonomous Response. This can be confirmed using ‘Reachability Testing’, which confirms the absence of factors that would prevent Autonomous Response actions being effectively taken.

Devices not in scope of coverage will not be monitored by Managed Detection and Response service. At minimum, Darktrace recommends the following coverage:

- / NETWORK:
  - Access (Call Home) to master instances expected to be covered by Managed Detection and Response
  - All critical issues identified within System Status resolved.
  - 75% of devices tagged for Autonomous Response
  - Running autonomous mode for external threat and significant anomaly models
  - Reachability has been tested and working on top 10 client subnets and top 10 Recent Traffic % subnets
  - Auto-updates to Autonomous Response models are appropriately configured
- / IDENTITIES and / CLOUD:
  - Running Autonomous Mode
  - All Autonomous Response Module running without errors and are authorized for Antigena
- / ENDPOINT:
  - All endpoint devices tagged for Autonomous Response
  - Running Autonomous Mode in external threat and significant anomaly models

- Endpoint Actions set to TRUE and a policy is set in cSensor Admin

When Autonomous Response is configured to operate in Human Confirmation (HC) mode, Darktrace SOC will include information on any pending Autonomous Response actions suggested by the models in the Managed Detection and Response alert sent to the customer's named contacts with the option to provide written approval for Darktrace SOC to activate the pending actions.

Degradation in the traffic received by Darktrace will affect the quality of service provided. Customers will be alerted to degradation in traffic through System Status alerts, which can be found on the / NETWORK UI System Status alerts are exportable to third-party monitoring systems and give customers the option to open a support ticket for further assistance to restore traffic flows should it be required.

4.3 Customer Responsibilities

Coverage of the Managed Detection and Response service is dependent on / NETWORK visibility and coverage. It is the Customer's responsibility to ensure and maintain that its deployment is sufficient to support proper Managed Detection and Response functionality. Darktrace recommends customers perform regular SPAN coverage and Autonomous Response reachability checks to make updates where necessary, and that these checks are also performed following any network changes.

Recipients and delivery preferences for Managed Detection and Response alerts are configured in the Customer Portal. Darktrace recommends that periodic checks are made to ensure Managed Detection and Response alert recipient details are correct.

We encourage customers to review the use of Darktrace device tags as utilized within the 'Enhanced Monitoring' models, as set out below. This list may be updated/changed via documentation on the Customer Portal at any time:

1. AD FS Server
2. Admin
3. Android Device
4. Conflicting User-Agents
5. Critical Attack Path
6. DNS Server
7. Darktrace Appliance
8. Domain Controller
9. Gateway
10. Internet Facing System
11. Mail Server
12. No Device Tracking
13. OT Engineer
14. Pentest
15. Proxy
16. Re-Activated Device
17. Security Device
18. Successful Poisoning Behavior
19. Unusual Connectivity Excluded
20. VoIP Activity
21. WSUS / SCCM
22. iPhone

4.4 Customer and Darktrace Roles

Role	Responsibility
Customer Roles	
Network/System Admin	(1) Ensure Darktrace / NETWORK coverage meets the minimum recommended coverage set out in section 4.2.

	(2) Perform regular checks of Darktrace SPAN coverage, Autonomous Response configuration and reachability testing. (3) Respond accordingly to System Status alerts to ensure optimal traffic quality and delivery . (4) Maintain call-home connectivity with Darktrace.
Customer Portal Primary User	• Administration of customer SOC contacts in the 'Client Management' section of the Customer Portal.
SOC Contacts	• Ensuring they have verified their Customer Portal accounts and set their communication preferences for SOC alerts. • Ensuring that they have the pre-set Darktrace TIR password which can be requested via the Customer Portal. • Any onward actions required upon receiving a Managed Detection and Response alert.
Darktrace Roles	
SOC Analyst	• Timely triage and investigation of Managed Detection and Response customer Enhanced Monitoring model breaches. • Conducting reviews of Autonomous Response activity associated to Enhanced Monitoring model breaches and taking designated Managed Detection and Response action . • Following investigation of an 'Enhanced Monitoring' breach, collation and timely delivery of / NETWORK information regarding potentially damaging cyber threats to a Managed Detection and Response customer. • Respond to feedback and/or requests for further assistance via Customer Portal tickets.
Regional SOC Manager	• Ensure sufficient analyst resource is available to provide coverage for the Managed Detection and Response service. • Owner of Managed Detection and Response Quality Control process. • Liaison with model developers to ensure that the 'Enhanced Monitoring' models are maintained for optimal detection capability.
Escalation Point	• In the event that Customer is not satisfied with the provision of the Managed Detection and Response Services (in accordance with this Service Definition), Customer may seek escalation to the following positions as appropriate: o Director of SOC Operations; or o Director of Analyst Operations. • Receives Customer issues and uses all reasonable endeavors to resolve the escalated issues. • Provides regular updates on escalated issue until resolution is reached.

5 Analyst Services

5.1 Service Features

Included within the Managed Detection and Response Service Bundle are the following Analyst Services:

- 1 Analyst Consultancy Session per quarter;
- 2 Operational Efficiency Report (OER) per annum; and
- Monthly SOC Service Reports.

5.2 Analyst Consultancy Sessions

5.2.1 Pre Analyst Consultancy Session

Subject to available resources, Darktrace will assign an available analyst for the time slot booked by Customers. Analyst Consultancy Sessions are made available once per quarter and must be agreed at least 10 working days in

advance. Should Customers cancel or move an Analyst Consultancy Session within 10 working days of the originally scheduled time slot, any rearranged time slot is subject to the same advance notice provisions.

Requests for Analyst Consultancy Sessions are managed via Customer Portal tickets. Darktrace recommends that periodic checks are made to ensure that Customer Portal account administration is up to date. Customers should specify their desired subject of the Analyst Consultancy Session in the Customer Portal Ticket at the point that the Session is booked, and the subject should not be adapted within 10 working days of the Session date.

The Analyst Consultancy Session may be conducted on any of the following subjects:

- Review of current alerting;
- Observations on current workflows;
- Review of potential model adjustments / optimizations;
- Bespoke Model Creation / Custom Use Case Developments; and
- Review of Autonomous Response Models and alerting volumes.

Ahead of the Session, it is recommended that the Customer complete the following training sessions: Threat Visualizer Part 1 – Familiarization, and Threat Visualizer Part 2 – Investigation. Darktrace may also require Customer to provide addition necessary information in advance of a Session to enable analyst consultants to prepare and maximize value from the Session.

5.2.2 Session Composition

An Analyst Consultancy Session consists of an interactive video call led by a Darktrace analyst consultant, who may be supported by a member of Customer's usual account team. During the Session the analyst consultant will access Customer's environment via their Darktrace User Interface. Each session may last for a maximum of two hours.

In order to ensure efficacy of the Session, Customer should ensure that there at least one active member of the Security team/user of Darktrace in attendance. There is no limit to the number of Customer participants that may join the Session and Customer is advised that Sessions cannot be recorded.

Notes of the contents of the call will be taken throughout and a summary of what was covered will be shared with the Customer after the Session via a Customer Portal ticket along with any relevant materials that were presented during the Session. No changes or edits to a deployment or live environment may be made by Darktrace during the Session.

The focus of the Sessions is intended to be centered on models, workflows, alert configuration and analysis. Any questions or analysis on integrations are to be handled separately by Customer's account team outside of the Session.

5.2.3 Post Analyst Consultancy Session engagement

All recommendations and reports following the Session will be shared via Customer Portal.

Post-session engagement between the customer and Analyst will occur over the dedicated Customer Portal ticket created for Analyst Consultancy Session. A writeup of each Session and applicable outcomes will be recorded and tracked via the Customer Portal ticket. After the Session, Customers maintain responsibility for all follow-up analysis and any remediation activity required, as designated by their own security/IT policies.

Any model or workflow suggestions will be shared via the customer portal, any model changed may be requested to be developed directly by Darktrace and put into experimental mode to assure performance ahead of putting in live. Customer must provide consent for Darktrace to make any model changes to Customer's environment, and Customer acknowledges that any such changes made by Darktrace with Customer's consent, are made at Customer's own Risk. Darktrace may advise against certain changes if it is believed to negatively impact the level and quality of services.

Customer acknowledges that Session Analysts will not be responsible for the ongoing monitoring of alerts during the contracted period that have been created or edited. Any alerts may be reviewed during Sessions, however, ongoing

daily alerting is covered by the Managed Detection and Response Service element of the Managed Detection and Response Service Bundle.

Once the Analyst Consultancy Session Customer Portal ticket has been closed, any ongoing communications with the analyst team must be done via the Darktrace Security Operations Support Service on the Customer Portal.

5.3 Operational Efficiency Reports OERs

OERs are made available to Customer once every 6 months in the form of an encrypted PDF sent to the email address(es) nominated by Customer. The OER will include a review of the Customer's deployment's enrichment, integrations and alerting, and will advise on appropriate thresholds on external alerting. The report may also contain metrics on the / NETWORK and AI Analyst model breaches to provide context to how the deployment is alerting. Also included will be a diagrammatic overview of the deployment in relation to the customer's security stack and a review of the / NETWORK models and number of breaches in the last month.

The OER will identify a set of objectives where it is recommended that Customer focuses their optimization efforts. Specific actions recommended to achieve those objectives will be provided in a separate document (referenced below) as these will be agreed on jointly with the customer.

Analyst Consultancy may build on OERs with the objective to: review workflows, review model performance, prioritize alerts, identify important threats; this will be assessed and adapted on a per customer basis. All sessions and reporting are provided with a view to ensure full capabilities within the Customer's Darktrace deployment are reached and to provide best-practice guidance and tailored recommendations.

5.4 Monthly SOC Service Report

Darktrace will also provide monthly Service Reports derived from the Managed Detection and Response service and the wider ecosystem of Darktrace's Managed Threat Detection Service, made available to the Customer via the Customer Portal. The SOC Service Report will consist of a PDF report that includes information specific to Customer, outlining the Managed Detection and Response alerts that have been escalated, as well as insight into incidents that were triaged, but did not generate a notification. The report will also provide broader contextual information Darktrace has observed across the entire Managed Threat Detection service in order to provide insight into the threat landscape for that month. An average report will consist of circa 11 pages as well as additional appendices, the number and length of which are determined by the number of alerts resolved and/or raised that month.

6 Assumptions

Darktrace will not be liable to provide Support Services with respect to a deployment which is faulty on the basis of:

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

NO ADVICE, ALERT, OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY CUSTOMER FROM DARKTRACE OR THROUGH OR FROM THE SUPPORT SERVICES SHALL CREDarktrace Security Operations Support ANY WARRANTY NOT EXPRESSLY STDarktrace Security Operations SupportD HEREIN OR IN THE MASTER SERVICES AGREEMENT. DARKTRACE SHALL NOT BE LIABLE FOR ANY ERRORS OR DELAYS IN THE CONTENT OR ALERTS AVAILABLE THROUGH THE SUPPORT SERVICES, OR FOR ANY ACTIONS TAKEN IN RELIANCE THEREON. THE CUSTOMER UNDERSTANDS AND ACKNOWLEDGES THAT NOT ALL ANOMALIES / INTRUSIONS MAY BE REPORTED.

Customer acknowledges that Darktrace's ability to perform the Managed Detection and Response service 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. 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.

Customer acknowledges that, prior to the Service Ready Workshop, the Darktrace deployment may not be configured to meet the minimum recommended standards set out in section 4.2, and agrees that Darktrace is not liable for any associated reduced operationality of the Managed Detection and Response service. After the Service Ready Period elapses, Customer acknowledges and accepts that Darktrace is not liable for reduced operationality of the Managed Detection and Response Service resulting from implementation issues identified by the Service Ready reports or otherwise.

Customers utilizing a cloud/hosted environment for their Darktrace deployment, acknowledge that these services are provisioned in accordance with Azure/AWS and as such, any outages or maintenance of this cloud infrastructure may affect service provision.

The review and analysis of Managed Detection and Response alerts is a discretionary exercise conducted by Darktrace SOC analysts on the basis of the data generated by: the coverage provided by Customer's Darktrace Product Offering; context provided by Customer to Darktrace; and Darktrace SOC's experience of the relevant threat landscape. Darktrace provides no warranties or representations as to the accuracy or reliability of the data, analysis, or recommendations provided by the Managed Detection and Response service and any conclusions, decisions, actions or interpretations of any recommendations provided as part of the Managed Detection and Response service are inferred or taken at Customer's own risk. To the fullest extent permissible by applicable law, Darktrace accepts no liability for any actions taken or inferences made by Customer.

Customer consents to Darktrace SOC having the ability to extend or activate both: (i) actions suggested by relevant Autonomous Response models; and (ii) POL actions, whether suggested by Autonomous Response models or otherwise. Customer acknowledges that POL actions impact the Customer's live environment and may result in activity being blocked. Darktrace shall not be liable for any damages caused to Customer, or any other party, as a result of extending or activating an action, regardless of whether such action was suggested by Autonomous Response modelling. Managed Detection and Response is delivered by Darktrace's global SOC using a follow-the-sun shift pattern. Accordingly, in the event that an Enhanced Monitoring Alert is received outside of Customer's jurisdiction's normal office hours, the Alert may be reviewed by a Darktrace SOC team member located in a different jurisdiction. A complete list of the jurisdictions that host SOC team staff can be found in Appendix 2 of the Master Services Agreement, found at https://darktrace.com/legal/master-services-agreement.

Any alert data that is transferred to a different jurisdiction to that of its origination, is done so in conjunction with the Darktrace Data Processing Addendum, a copy of which can be found at https://darktrace.com/legal/master-services-agreement.