DARKTRACE

# Service Description: Managed Threat Detection

## Service Features

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

## 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 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, the number of alerts sent to Darktrace SOC is rate limited.

Darktrace SOC works closely with our model development specialists to continually review and revise the Enhanced Monitoring models used for the Managed Threat Detection 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, to be used as similar logic for their own alerting purposes. Darktrace may make bespoke changes to an individual customer's 'Enhanced Monitoring' models to improve model proficiency for the customer's Managed Threat Detection 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 inflight 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.

## Alert Details

In the event an anomaly triggers the Enhanced Monitoring parameters and is deemed sufficiently high-risk, Managed Threat Detection alerts are delivered to customer's named contacts via an email attachment secured by a password. A Managed Threat Detection 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.

In the event that, following investigations that an anomaly 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 model investigated. This will include an indication of whether an alert has been raised. These comments allow customers to identify models that have been investigated by the Managed Threat Detection service.

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

## Requirements

Managed Threat Detection is only available to customers using / NETWORK and/or / IDENTITES. If configured within / NETWORK, Managed Threat Detection can also provide coverage of / OT, / CLOUD, / IDENTITIES and / ENDPOINT.

Managed Threat Detection 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 appliance operating Call-home will attempt to establish a secure SSH 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 TCP Port 22 or HTTPS/443 with SSL wrapping.

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

Customers must enable “Auto Update Models” in the Model Updates section on the sysconfig page of the / NETWORK UI to ensure that the ‘Enhanced Monitoring’ models are kept up to date.

Degradation in the traffic received by Darktrace will affect the quality of service provided. Customers will be alerted to degradation in traffic through Sys Status alerts, which can be found on the / NETWORK UI and will contain information and guidance to assist in restoring traffic flows.

Customer Responsibilities

Coverage of the Managed Threat Detection service is dependent on / NETWORK visibility so Darktrace recommends customers perform regular SPAN coverage checks and make updates where necessary, and that these checks are also performed following any network changes.

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

We encourage customers to review the use of Darktrace model tags as utilized within the ‘Enhanced Monitoring’ models. We encourage customers to review the use of Darktrace model tags utilized within the ‘Enhanced Monitoring’ models. This list may be updated/changed **via documents uploaded to 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 Behaviour
19. Unusual Connectivity Excluded
20. VoIP Activity
21. WSUS / SCCM
22. iPhone

Customer and Darktrace Roles

| Role | Responsibility |
|---|---|
| **Customer Roles** | |
| 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.<br>• Ensuring that they have the pre-set Darktrace TIR password which can be requested via the Customer Portal.<br>• Any onward actions required upon receiving a Managed Threat Detection alert. |
| **Darktrace Roles** | |
| SOC Analyst | • Timely triage and investigation of Managed Threat Detection customer Enhanced Monitoring model breaches.<br>• Following investigation of an 'Enhanced Monitoring' breach, collation and timely delivery of information regarding potentially damaging cyber threats to a Managed Threat Detection customer.<br>• 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 Threat Detection service.<br>• Owner of Managed Threat Detection Quality Control process.<br>• 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 Threat Detection Services (in accordance with this Service Definition), Customer may seek escalation to the following positions as appropriate:<br>o Director of SOC Operations; or<br>o Director of Analyst Operations.<br>• Receives Customer issues and uses all reasonable endeavors to resolve the escalated issues.<br>• Provides regular updates on escalated issue until resolution is reached. |

Post-Alert Support

Although Darktrace SOC analysts may include suggested actions within a Managed Threat Detection 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 Threat Detection alerts using the associated Managed Threat Detection ticket generated on the Customer Portal.

Upon request, Darktrace SOC can assist with further analysis of an investigation generated by a Managed Threat Detection alert. Customers are encouraged to reach out to Darktrace SOC using the Managed Threat Detection 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.

Assumptions

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

(i) improper use, site preparation, or site or environmental conditions or other non-compliance with applicable Documentation or these terms;
(ii) failure or functional limitations of any non-Darktrace software or product impacting systems receiving Darktrace Hardware Support Services;
(iii) malware (e.g. virus, worm, etc.) introduced by Customer;
(iv) modifications or improper system maintenance or calibration not performed by Darktrace or authorized in writing by Darktrace;
(v) fire damage, water damage, accident, electrical disturbances, transportation by Customer, or other causes beyond Darktrace's control; or
(vi) 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 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 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 Threat Detection 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.

Darktrace aims to notify Managed Threat Detection customers with at least 72hrs notice of scheduled maintenance that is expected to exceed more than 1 hour in duration and would affect service delivery. Darktrace aims to notify customers as soon as reasonably possible for unexpected outages expected to exceed more than 1 hour in duration and would affect service delivery.

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.

Managed Threat Detection 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.