DARKTRACE

Service Description: Security Operations Support

Service Features

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

Analytical Assistance

Customer can enter requests for analytical assistance on threat investigations direct from the Darktrace UI or via the Customer Portal. This includes, but is not limited to; threat investigation guidance, recommendations and suggested modifications to models, detailed explanations for Darktrace findings. For queries requesting analytical assistance, call home will be required.

All Security Operations Support queries are answered by analysts working in the 24/7 Darktrace SOC. This team is resourced by experienced Darktrace analysts who will have received and passed cross-platform training on the analytical uses of the Cyber AI Loop technologies.

To open a Security Operations Support ticket from the Darktrace / NETWORK UI, navigate to Menu>Help>Security Operations Support.

In the event customer does not have Call Home, Security Operations Support tickets can be raised on the Customer Portal.

All Security Operations Support requests are converted into Security Operations Support tickets, which are visible to the customer on the Customer Portal. New and existing Security Operations Support tickets, regardless of UI/portal origin, are assigned to Darktrace SOC analysts in order of receipt using the ticket management system hosted on Darktrace's Customer Portal.

Requirements

Security Operations Support is dependent on the granting of Call Home access for the analysts to be able to interact with the Offering.

Access to the Security Operations Support service via the Darktrace / NETWORK UI 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 a Security Operations Support request has been made.

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 TCP Port443.

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

Customer Responsibilities

Analysts can only advise on activity and events within Darktrace visibility so customers are advised to perform regular SPAN coverage checks and make updates where necessary, and that these checks are also performed following any network changes.

All customer contacts with a validated Customer Portal account are able to access the Security Operations Support service. Darktrace recommends that periodic checks are made to ensure that customer portal accounts are kept up to date.

Customer and Darktrace Roles

Role	Responsibility
Customer Roles	
Customer Portal Primary User	• Administration of customer portal accounts in the 'Client Management' section of the Customer Portal
Customer Portal Users	• Ensuring they have verified their Customer Portal accounts and set their security questions. • To create new, and respond to existing, Security Operations Support requests
Darktrace Roles	
SOC Analyst	• Timely triage of all customer Security Operations Support requests • Collation and timely delivery of information in response to customer raised Security Operations Support requests
Regional SOC Manager	• Ensure sufficient analyst resource is available to provide coverage for the Security Operations Support service. • Owner of Quality Control process.
Escalation Point	• In the event that Customer is not satisfied with the provision of the Security Operations Support 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.

Contact

For urgent enquires 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 Security Operations Support 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 Security Operations Support customers with at least 72hrs notice of scheduled maintenance on the Customer Portal 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.

Security Operations Support is delivered by Darktrace's global SOC using a follow-the-sun shift pattern. Accordingly, in the event a Customer raises a ticket outside of that Customer's jurisdiction's normal office hours, the ticket may be reviewed by a SOC team member 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 data attached to the ticket 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.