Darktrace Analyst Services

Darktrace is committed to ensuring that you receive the maximum value from our world-class Self-Learning AI technology and expert analysts. In order to best support you, our service options can be customized to uplift and and extend your security and IT teams.

Services can be delivered by Darktrace's Cyber Analysts, experts in threat analysis and cyber intelligence, or Darktrace Certified Partners. Most importantly, these offerings are crafted based on experience across all sizes of companies and sectors to give you a custom fit.

24/7 Proactive Threat Notification

Darktrace's Security Operations Centers (SOC), located in Cambridge, San Francisco, and Singapore, provide you with around-the-clock coverage of significant incidents identified within your digital ecosystem, as flagged by your Darktrace deployment. Manned by our world-class Darktrace Cyber Analysts, this service notifies you of unusual activity or deviations in behavior which may be indicative of an in-progress attack. These incidents are rapidly triaged on demand, and our Cyber Analysts will provide you with the information you need to take action on events as they occur.

Proactive Threat Notifications (PTN) ensure that high-fidelity incidents, which are strong indicators of an emerging attack, are funneled directly into the global Darktrace SOC for triage and assessment by our expert team of Cyber Analysts.

The alerts monitored by Darktrace as part of the PTN service can be identified by the Enhanced Monitoring tag within the Enterprise Immune System and can be viewed by filtering in the Threat Visualizer and Model Editor. The Enhanced Monitoring tag also enables you to see exactly which model breaches have been escalated into the SOC for triage.

Our Research and Development team continually evaluate and update our PTN service to ensure that Darktrace is investigating the highest priority breaches and are able to quickly respond to attacks of all kinds - from traditional known attacks, to new and never-before-seen threats.

Once a PTN is promoted into the Darktrace SOC it will be triaged by one of our global Cyber Analysts. For more complex cases, the Darktrace SOC has access to senior Level 3 analysts across our global analyst workforce. The decision on alerting may involve a number of analysts working together to come to an informed decision as to whether your organization is under a direct and immediate threat.

Note that not all alerts are triaged, only incidents that are highly indicative of attack are marked with the Enhanced Monitoring tag and will be triaged by PTN analysts.

Should Darktrace find strong evidence of attack during the triage phase, your team will be contacted immediately and provided with the intelligence ascertained in order to take action. Darktrace would suggest that any PTN alert be treated as high priority. Fully triaged alerts will be encrypted using a shared secret key and emailed to a named distribution list within your organization. You can also receive automated telephone calls and/or SMS messages if a PTN email alert has been issued. You can configure SOC contacts and messaging delivery methods via the Customer Portal in your account preferences.

> "Our team can often be stretched thin. The direct emails and calls we've received since subscribing to Darktrace's PTN service has empowered us with the necessary intelligence to take immediate action."
>
> CISO, Better.com

24/7 Ask the Expert

Accessible from within the Threat Visualizer and Customer Portal, Ask the Expert (ATE) is a feature that can be enabled so that you and your security team can send queries to a Darktrace Cyber Analyst for expert assistance during live threat investigations. You will receive rapid feedback on new or advanced threats in your environment.

Accessing ATE via the Threat Visualizer gives you the ability to drag and drop graphics and traffic flow data into queries. This method of support enables your team to work collaboratively with Darktrace Analysts on a wide range of topics. When a Cyber Analyst responds to an ATE question, the answer will be available via 'Help -> View Questions' in the drop-down menu. These can also be seen in the Customer Portal.

There is no limit to the number of queries you can generate with ATE, but at times the Cyber Analyst may redirect you to internal training or technical operations teams if the question is less about analysis and more about software functionality. Software/Hardware Support services and feature requests must still be raised via the Customer Portal.

All ATE queries are queued for access to the global Darktrace Cyber Analyst team. While ATE is not a direct chat feature, if you are facing a real-time attack, Darktrace will prioritize access to the SOC and provide close support and rapid feedback during the initial investigation to ensure you have access to the data and intelligence generated from the Darktrace Immune System platform.

"Staff are super supportive and knowledgeable...their amazing support team is always eager to help and answer any questions."

Senior IT Specialist, Media

Service Delivery and Customer Data

Darktrace services are supplied by an in-house team of Cyber Analysts across our global SOC team. Access to our 24/7 services will depend upon the subscription agreements in your contract. The PTN service requires a standard Call Home connection from your master appliance to the Darktrace Management Center in Cambridge, UK. Darktrace provides for and monitors full audit logging from the Darktrace Management Center to record actions completed by Darktrace employees during the execution of the contracted services. Darktrace employees are required to give audited reasoning as to why they are accessing any given account before being granted an access token.

The service offerings available require analysis and reporting to occur outside of the Darktrace platform.

All data entered into Ask The Expert, both from your employees and the Darktrace Cyber Analyst team, is stored inside the Darktrace Customer Portal which is hosted by Darktrace in the Darktrace Management Center. Closed tickets remain in the portal archive for your review.

Enhanced Monitoring model breach data for Proactive Threat Notifications will be pulled back into the Darktrace Management Center and rendered in the Darktrace SOC dashboard. Analysts will review this data and log into your deployment to conduct further triage. Should a breach warrant an immediate threat alert, the analyst will send their findings to you, as detailed above. Model breach data associated with the alert, and reports that have been issued to you, are retained in the Darktrace SOC in case of review.