

AT A GLANCE:

- 24/7 Managed Detection & Response
- SOC investigation and action on high-priority Darktrace alerts across network, cloud, OT, endpoints and SaaS
- Regular feedback to optimize your deployment and workflows
- On-demand expert analyst support at every stage



Maximize your cyber defenses with wrap-around expert support

Boost your defenses with expertise at every level

Darktrace Managed Detection & Response is a wrap-around service that allows your team to focus on security outcomes rather than managing the tool day-to-day. Our global SOC triages, investigates and can escalate response actions on the highest-priority alerts in your Darktrace environment (across network, cloud, OT, endpoints and SaaS applications), buying your team precious time to coordinate a remediation plan while the threat is contained. Alongside 24/7 SOC support using a follow-the-sun model, our analysts are available for queries round-the-clock, as well as regular review sessions to ensure your operational excellence. You'll also receive monthly reports from our SOC, tracking the performance of your products, contextualised against insights into the wider threat landscape.

Why Darktrace?



AI that is trained on YOUR business data

Darktrace's unique Self-Learning AI learns from your data to understand what constitutes 'normal' for everyone and everything in your business, to catch novel cyber-threats other tools miss



Expert insight

Darktrace's global team of 100+ cyber analysts are experts in threat analysis and containing attacks, bringing a breadth of real-world knowledge and field experience to augment your organization



Extensive experience

Our deep expertise is gained from thousands of deployments globally across many industries and sectors, enabling us to provide you with a premium service

Tailored to your challenges

Ongoing alert management

Reduce the time your internal SOC spends triaging and investigating alerts, allowing them to focus on high-level strategic work

Latency between receiving alerts and taking human action

A 24/7 mechanism to contain threats buys security teams extra time to coordinate a response

Fast-moving incidents

Minimize time spent investigating and documenting a potential incident, shifting the focus to remediating and removing the threat

Maintaining 24/7 SOC coverage

Plug resource gaps in your security team with the expert investigative power of the global Darktrace SOC

Address skills shortages

Get regular training and recommendations from Darktrace experts to upskill your team and fine-tune your deployment

What Darktrace delivers:

Managed Detection & Response

Darktrace's 24/7 SOC monitors your DETECT environment across network, cloud, OT, endpoints and SaaS applications for significant anomalies indicative of an attack, and conducts investigations to alert you to potentially severe incidents. The SOC likewise reviews RESPOND measures related to the incident for an extra layer of security, with the power to escalate threat containment actions and provide additional context while your internal security team remediates the threat.

Ask the Expert

With 24/7 access to world-class analysts, your security team can send unlimited queries if they need assistance during live threat investigations – or even during day-to-day operations. Draw on Darktrace's expert guidance to work through a problem, ensuring you're benefiting from their advanced product knowledge and wealth of threat hunting experience.

Operational Efficiency Reports

Twice a year, our analysts will review the status of your deployment and deliver a report outlining trends in your DETECT, RESPOND and AI Analyst alerts, high-hitting devices, and how your deployment is alerting in relation to defined attack phases.

The report will provide consultancy insight with objectives and recommendations for optimizing and tuning your deployment for maximum operational efficiency, as well as recommendations to improve your overall cyber security hygiene and posture.

Quarterly Analyst Darktrace Managed Detection & Response Review

Following on from the recommendations in your Operational Efficiency Report, one of our analysts will meet with you quarterly to ensure you are reaching the full capabilities of your Darktrace deployment. As an external expert in the tool, they'll offer best-practice and tailored advice on streamlining your workflows, prioritizing alerts, model optimization, potential integrations, threat hunting and developing custom use cases.

Regular Darktrace Managed Detection & Response Service Report

You'll receive a monthly report from our SOC outlining how Darktrace Managed Detection & Response is performing in your environment – including a summary of all alerts raised as well as those that our analysts resolved – to give you full transparency over your service.

We'll also provide optimization recommendations and share insights from across our customer base so you're up-to-date with recent trends in the threat landscape and how you compare.

'Service Ready'

Once you join the service, our Delivery team will run a service ready check on your deployment and make recommendations on findings to ensure you'll get the most out of Darktrace Managed Detection & Response.



Darktrace Services give us the **peace of mind** that our business is **protected 24 hours a day, 365 days a year**, so even when we're asleep someone is looking after us."

/ Operations Director, Chemical Manufacturing

About Darktrace Services

Darktrace is committed to ensuring that you receive the maximum value from our world-class Self-Learning AI technology and expert analysts. Our bespoke service options can be customized around Darktrace's Cyber AI Loop to uplift and augment your security teams. Services are delivered by Darktrace's dedicated Cyber Analysts, Cyber Technicians and our 24/7 SOC operation, comprised of experts in threat analysis and risk mitigation. Most importantly, these offerings are crafted based upon our extensive experience working with thousands of diverse customers – it is this expertise that allows us to provide services that are tailored for your organization. **Terms and conditions apply; for additional information about this service, please refer to the service definition.**



Scan to LEARN MORE