

Optimizing Darktrace Operations



KEY BENEFITS:

- Learns normal 'on the job' to detect unknown and unpredictable cyber-threats
- Neutralizes attacks at machine speed and with surgical precision
- Autonomously investigates security incidents, reducing time to triage by up to 92%
- Offers unified and adaptive defense across the entire workforce and business

Workflow Models for Diverse Security

Darktrace is a versatile platform that can be used in a number of different ways depending on the size and resources of the security team in question, as well as the nature of the environment that is being monitored.

This guide reveals how to optimize Darktrace operations, whether a team has five minutes a day to use the platform's core features or thirty minutes a day to take advantage of more advanced functions.

Layer 1: Managing Resident Threats

Cyber AI Analyst: Augmenting the Team With Autonomous Investigations

When only a short amount of time can be allocated to the Darktrace interface, the most critical capability to leverage is Cyber AI Analyst, which allows security teams to immediately see the most significant threats happening in real time.

The technology pulls together related events into a clear Incident Report, including an AI-generated natural language summary and a visual timeline. Security teams will not need to spend too much time on each incident – they will see immediately if it is a big threat like ransomware, data exfiltration, or a malicious insider attack.

Incident Reports include a clear graphic pointing to where the threat sits in the kill chain. Several attack phases indicate a large threat that needs immediate attention. Automatically generated Incident Reports are available via the Cyber AI Analyst view in the Threat Visualizer or on the Cyber AI Analyst screen in the Darktrace Mobile App.

While Incident Reports are always created for the most critical threats at any one time, investigations can be applied on demand to any event of interest by selecting a device or user and clicking the 'Investigate' button. This provides the ability to easily confirm assumptions about suspicious activity, proactively threat hunt, effortlessly check on HR watchlists, or even help new starters on the security team understand how to pull together an investigation.

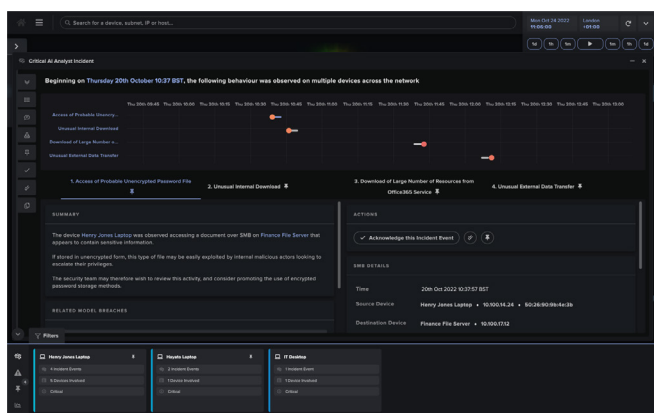


Figure 1: Cyber AI Analyst reports on the full scope of an incident, including attack chain phases

Cyber AI Analyst autonomously investigates every threat detected and highlights the highest-priority incidents at any one time, ensuring teams see what needs attention right away.

Cyber AI Analyst can be integrated with tools across the security stack, allowing investigations to be triggered based on data from third-party sources like CrowdStrike or Carbon Black. The rich context and insights of Incident Reports can additionally be exported to SIEM, SOAR, or ticketing systems to enhance existing workflows.

Enhanced Monitoring: Strong Indicators of Attack

Another key feature that teams can easily take advantage of is the Enhanced Monitoring model view.

Based on a bespoke set of parameters for each organization, they enable tailored defense of particularly sensitive data and vulnerabilities. When triggered, Enhanced Monitoring models are strong indicators of attack that immediately highlight to security teams the most heavy-hitting threats.

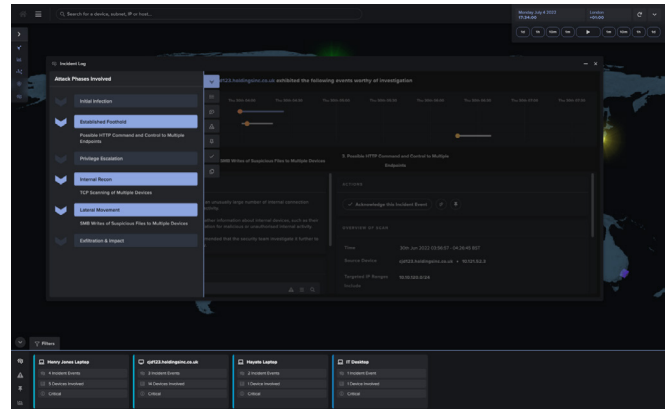


Figure 2: Cyber AI analyst attack phase incident log.

Layer 2: Analyzing Imminent Threats

When an analyst has additional time – even up to 15 minutes – they may wish to look at imminent threats: those that may soon become serious issues but are not causing immediate, widespread damage.

To start with, an analyst can filter the Threat Tray to review the devices that have the highest anomaly scores and may be associated with multiple instances of unusual activity. This quick look lets team members easily understand the top offending devices for a chosen time period and provides a good overview of what is happening.

For a different perspective, the top scoring model breaches can also be reviewed. Depending on risk appetite, this may be the threats in the top 15% priority level or it may be closer to 25%. Similarly, the Threat Tray can also be filtered by specific attack phases depending on business priorities: for example, analysts can search specifically for all instances of lateral movement or internal recon.

Layer 3: Discovering Future Threats

When an analyst has a bit more time to use Darktrace, they may wish to conduct in-depth threat hunts, investigate all model breaches, and perform granular analysis by taking advantage of features like Advanced Search and packet captures.

Investigating breaches with a lower threat score will allow the security team to identify early indicators of compromise and reduce the risk of future threats. This method of examination can also be used to look for and improve on cyber hygiene or regulatory compliance issues. For example, analysts can search through lower-level breaches to identify unencrypted password storage or Google Cloud being used where it is not compliant.

For teams with more time or resources, model optimization can be another crucial feature for getting the most value out of Darktrace. Model optimization allows security teams to adjust Cyber AI detections based on business needs or risk appetite,

or other factors analysts may wish to focus on. While this allows for customization towards the particular goals of a team, it is not a necessary action to receive the benefits of Darktrace's leading autonomous threat detection, investigation, and response.

Autonomous Response: The Machine Fights Back

Powered by self-learning Cyber AI, Darktrace RESPOND is the first and only solution that can interrupt attacks at machine speed and with surgical precision, even if the threat is highly targeted and entirely unknown.

Every second, Darktrace RESPOND stops an emerging cyber-attack – making it a critical tool for small and big security teams alike. The first step on the journey towards fully autonomous defense is setting up Darktrace RESPOND to react to the most critical threats.

The agility and accuracy of the technology allows even lean teams to effectively manage fast-moving, unpredictable attacks as they arise. Once RESPOND is set up to autonomously neutralize the highest-priority threats, teams can expand response actions to other detection cases – perhaps using Human Confirmation Mode.

In this mode, approval is requested from a human operator before action is taken. While using Human Confirmation Mode, analysts can gather various metrics to better understand their digital business and their optimal use of Darktrace RESPOND. For some teams, setting up RESPOND to match business needs may mean only enabling Active Mode – in which action is taken autonomously – on the weekends or just in certain areas of the organization.

Third-party tools, such as firewalls, can also be integrated, allowing AI-driven responses to be triggered via other solutions throughout the security stack.

As teams expand their capabilities and have increased availability, Darktrace RESPOND can be used to enforce corporate policy and regulatory compliance goals. For instance, RESPOND can stop unencrypted FTP from leaving the network, neutralize an email containing malicious links, and pause an employee’s non-compliant use of a SaaS application.

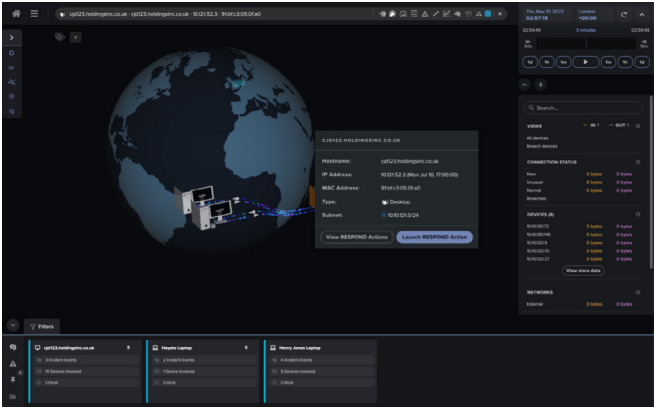


Figure 3: Darktrace RESPOND stopping an in-progress threat.

Operationalizing Darktrace: A Spectrum of Use

The diagram below describes the level and type of interaction with Darktrace that is recommended for teams of varying resources and time.

Layer 1 applies to small teams or those with limited time, who will find the most value in Cyber AI Analyst and Enhanced Monitoring models to manage resident threats that need immediate attention. These teams can also easily set up Darktrace Antigena to ensure Autonomous Response capabilities align with their most critical business needs.

Teams that can afford to be more proactive in their use of Darktrace can scale to Layers 2 and 3, addressing imminent and future threats. These teams may make use of the filter function to identify top-scoring threat types, top offending devices, and the attack phase seen. They might also move towards investigating detections with a lower threat score, often for the sake of analyzing cyber hygiene or compliance issues and leveraging model enhancement options. These teams might also wish to customize RESPOND’s actions at a more granular level, optimizing response actions and use cases based on more nuanced business needs.

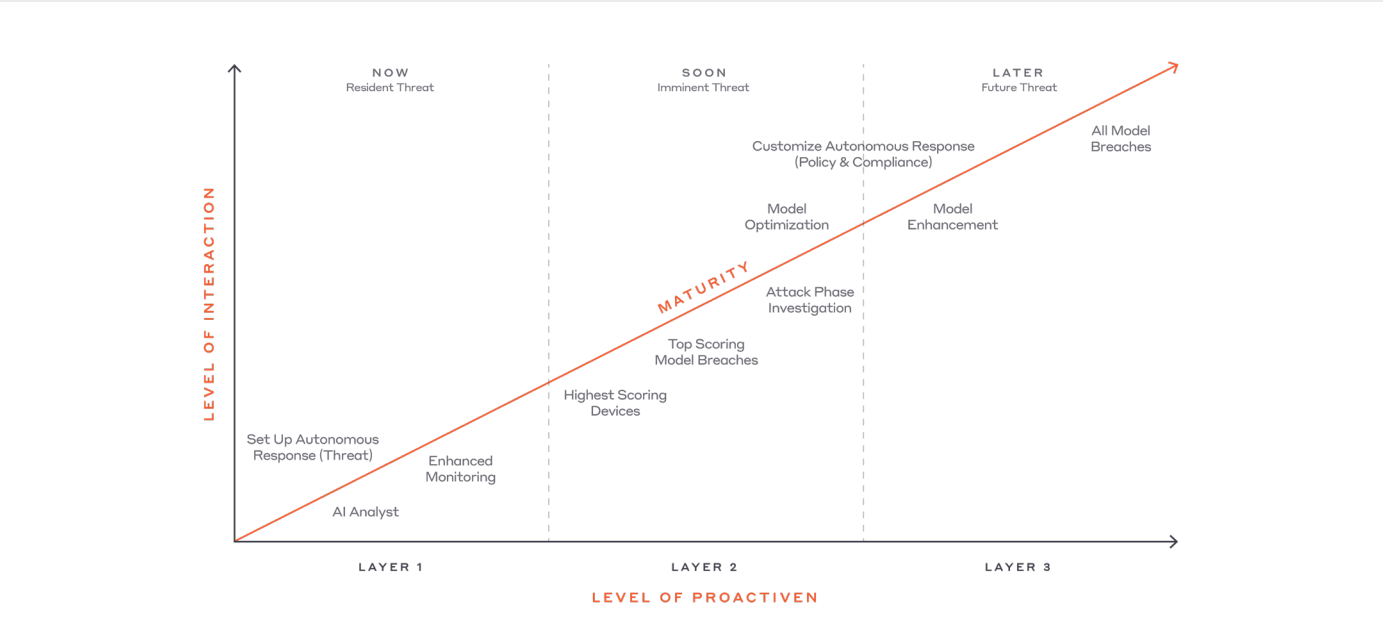


Figure 4: Teams of varying resources and time can leverage Darktrace’s technology in different ways to get the most value from the AI.

Cyber AI on the Go: The Darktrace Mobile App

The Darktrace Mobile App lets security teams protect the dynamic workforce and monitor their entire digital ecosystem on the go. Teams get real-time threat notifications, control over RESPOND's Autonomous actions, and can investigate the most significant incidents with Cyber AI Analyst - all from their phone.

Self-Learning Cyber AI gives security teams enterprise-wide coverage that evolves and grows with the business, and with our Mobile App, teams can stay ahead of any threat that emerges. Use the App to:

- Examine Cyber AI Analyst incident summaries
- Discover device and model breach details around emerging threats
- Add and review comments on anomalous events
- Pin significant incidents or email to a colleague
- View and adjust RESPOND's Autonomous actions

Easy Win Integrations

The Darktrace platform was designed with an open and extensible architecture that seamlessly integrates with existing investments.

Customers can enhance and extend their Darktrace deployment via one-click integrations, including the ability to immediately extend coverage to new cloud services, enrich the platform's analysis with new sources of log ingestion, and activate coordinated Autonomous Response via integrations with other security defenses. If the chosen provider is not listed on Darktrace's configuration page, custom templates make it easy to set up bespoke integrations.

LDAP: Authentication and Enriched Visibility

Integration with LDAP servers, such as Active Directory, can support authenticated access to the Threat Visualizer, as well as enrichment of Darktrace visibility by providing additional LDAP attributes for users. Darktrace also provides the option to create LDAP group tags for use in threat modeling. Current customers can see the integrations guide here.

EDRs: Enhanced Endpoint Protection

Darktrace can ingest EDR alerts as weak indicators that inform Cyber AI's analysis across the business. EDR alerts can also trigger Cyber AI Analyst investigations, without the need for an underlying Darktrace detection. Current customers can see the integrations guide on alerting options here.

VPN and Zero Trust Technologies: Extended Workforce Coverage

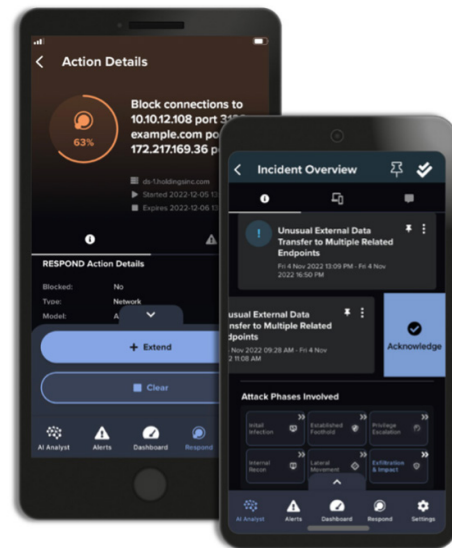


Figure 5: The Darktrace Mobile App monitors the entire digital estate on the go

By integrating with VPN and zero trust services, Darktrace can extend its visibility across an increasingly distributed workforce. Low-effort native integrations and custom templates are available for any service in this area. Current customers can see the access control integrations guide here.

Firewalls: Autonomous Response and Added Context

Darktrace Antigena can trigger Autonomous Response actions via integrations with firewalls and preventative controls for attacks that have gotten through. Darktrace can also ingest logs from firewalls and network devices to extend visibility as needed. Current customers can see the integrations guide here.

SIEMs and SOARs: Sharing AI Insights

Native integrations via API and syslog allow Darktrace to feed AI detections and Cyber AI Analyst incidents to SIEMs for analysis and correlation, as well as to SOAR solutions to trigger response playbooks. Darktrace can also poll SIEM and SOAR solutions to ingest enrichment data, and SOAR playbooks can be configured to trigger custom models and Cyber AI Analyst investigations in Darktrace.

Single Sign On: Seamless Access

For ease of use, Darktrace natively supports authentication and access via SAML 2.0 Single Sign On.

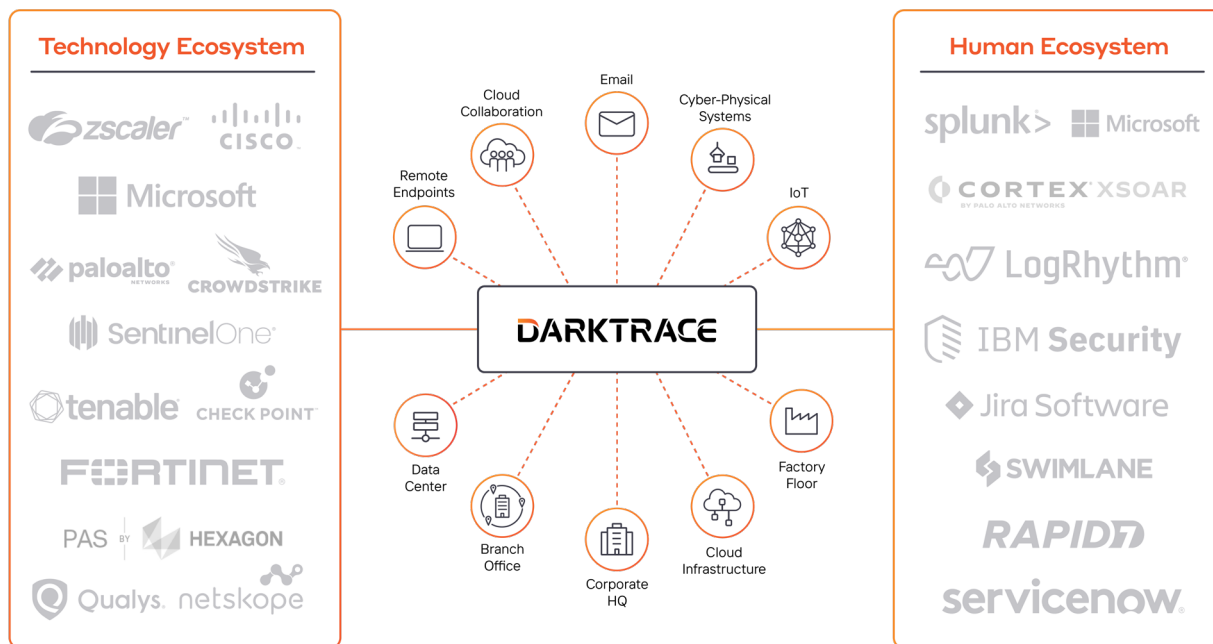


Figure 6: Darktrace integrations

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted in over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,800 organizations globally from advanced cyber-threats.



Scan to
LEARN MORE