DARKTRACE

Darktrace / Incident Readiness & Recovery

Prepare, restore and harden against cyber attacks

Defenders must be ready

Organizations face a constantly changing cyber security landscape with increasingly sophisticated attacks, exacerbated by the professionalization of adversary groups and the new adoption of AI to enhance their tactics and techniques. If successful, compromises have a bigger capacity than ever to cause large operational, financial, and reputational damages.

Yet many teams are not prepared. Although security budgets are increasing, organizations still experience human resource constraints, process deficiencies, and inadequate technical solutions that fail to meet these requirements. In some cases, businesses do not have an Incident Response (IR) plan at all.

Consequently, SOC teams typically have a lag before their response, leading to a higher dwell time and bigger overall costs. For example, only 15% of the total cost of ransomware is affiliated with the ransom itself. The rest is from business interruption.[1]

It's crucial that organizations can respond and recover earlier, so teams need to be practised.

Business benefits

Maximize business confidence in your security
Show resilience against attempted compromises and evidence of robust testing practices with incident simulations

Reduce impact of an adversary
Detect, respond and recover faster and more effectively with bespoke AI playbooks unique to each incident and your environment

Keep up with urgent reporting standards
Automated reporting outlines incident details, actions taken and technology health for any necessary audience

Separate obstructive departmental barriers
Encourage collaboration between security, GRC, legal and other stakeholders with the Communications Center

Optimize expensive security stack
Reduce siloed services or tabletops with an integrated IR solution with foundations in detection, response and investigation

1 https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/

Aligning preparation and response

Darktrace / Incident Readiness & Recovery goes beyond traditional security stacks by empowering teams with proactive measures to minimize disruption earlier in the attack lifecycle. Leveraging the AI Recovery Engine, Darktrace provides a deep understanding of your environment and each threat to chart the most effective path to incident resolution.

Responder performances are optimized through simulated tests that ensure confidence that an organization's technologies, processes and people will work effectively in a real incident. With a continual assessment of human and technology readiness, Darktrace ensures your team is always prepared to adapt and respond effectively to modern threats.

Seamlessly integrating collaboration and communication tools, Darktrace enables teams to maintain focus and operational continuity, even under the pressures of a real compromise.

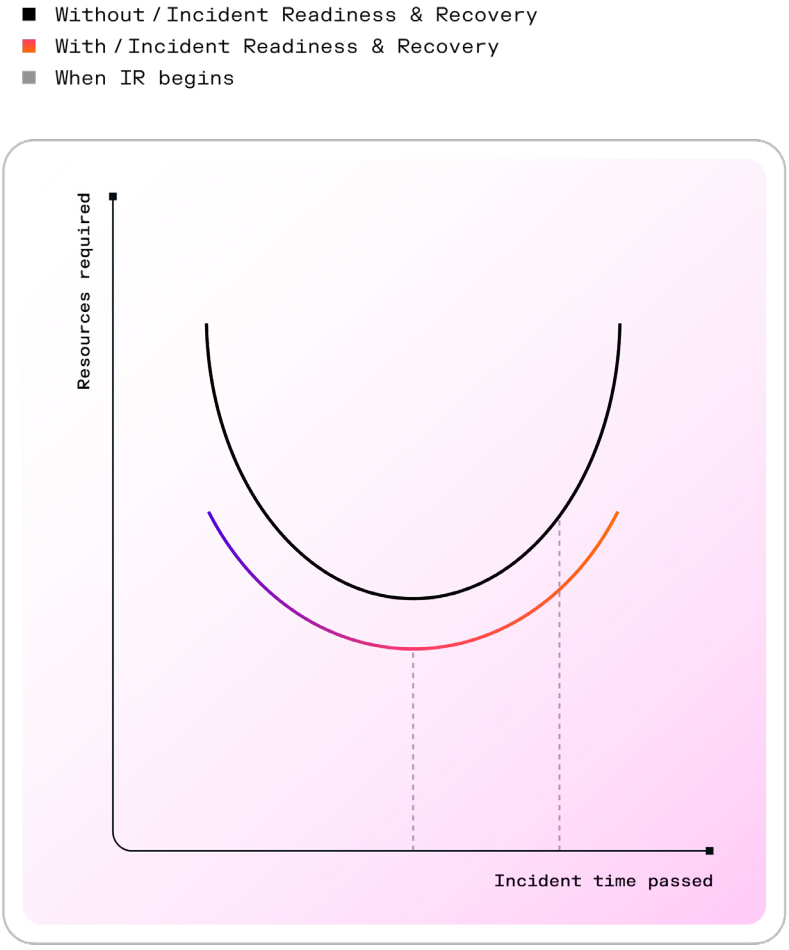


Figure 01: Close integration with Darktrace's native detection and automated analysis capabilities allow Incident Readiness & Recovery users to introduce traditional IR techniques sooner and more easily, without the need to confirm and declare a formal incident first. Should an incident then be confirmed, the organisation is in a much better position resulting in lower overall impact.

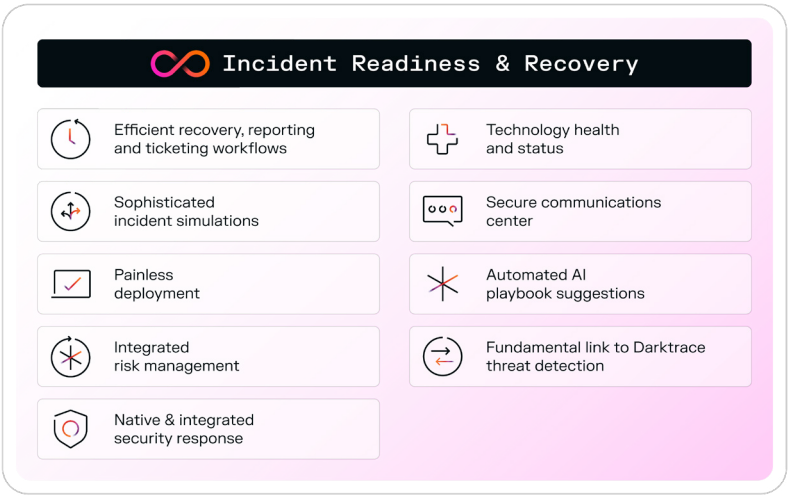


Figure 02: Darktrace unifies and automates critical IR and readiness operations

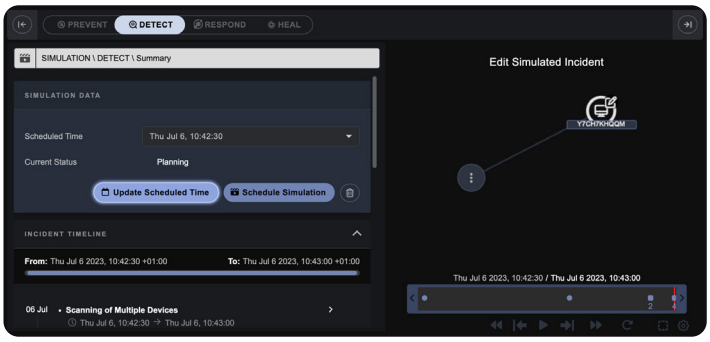
Key Capabilities

Leverage incident simulations based on real-time threats

Build team confidence by mapping scenarios based on attacks seen in-the-wild into your current environment. Test, improve and sharpen existing IR functions to their best version, using a breadth of sophisticated incidents beyond what can be simulated in other products.

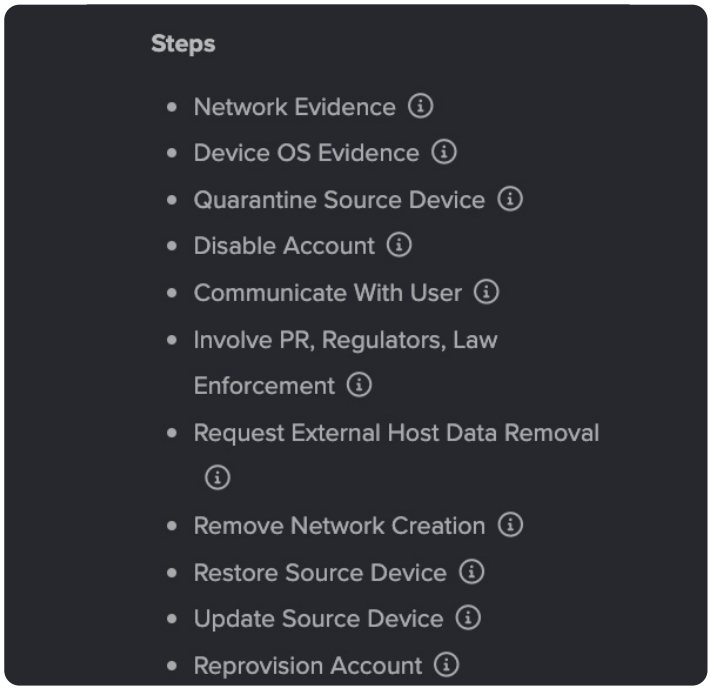
Teams can extract quicker time-to-value from new hires by training them on detailed scenarios in the context of your own security tooling and real environments with interactive feedback allowing managers to review the prioritization and speed of response and recovery activities that could have improved the outcome of the incident.

Unlike tabletops, owning incident simulation capabilities that can be set-up and run from within your own security dashboard allows exercises to be run as frequently as desired to build investigation and response habits. This enables both a continuous proactive approach ahead of a threat and easier reactive practice following a response to a real incident.



Minimize impact and damage during live compromises

Darktrace's industry-first AI-powered recovery engine gives security teams easier, efficient incident response workflows to minimize risk and damage during live compromises.



Only with Cyber AI Analyst bringing an initial understanding of what has happened and the setting it has occurred in, can Darktrace / Incident Readiness & Recovery adapt its playbooks to evolving threats. Unlike pre-defined playbooks, your suggested playbooks and actions are refined based on the exact events that have taken place on each affected asset.

This ensures that security teams maintain a position of best guidance as their business or incident changes. This will speed-up the time analysts take to gather information, assess, and perform the most effective actions. 'New Events' are updated and announced in real-time so responders always know how their incident is evolving and can adapt accordingly. Recently recovered assets are closely monitored for further signs of compromise, ensuring resilience for the next threat.

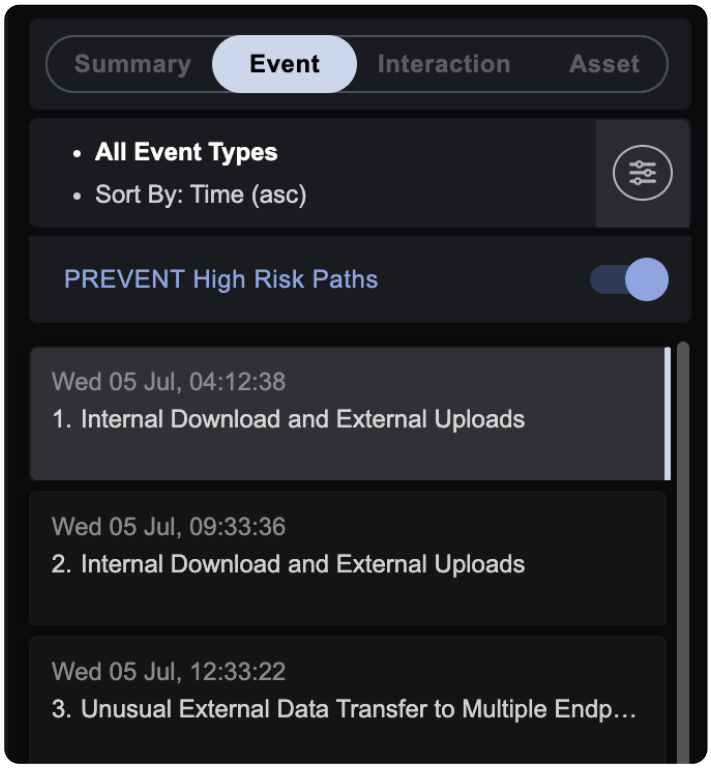
Develop effective post-response workflows

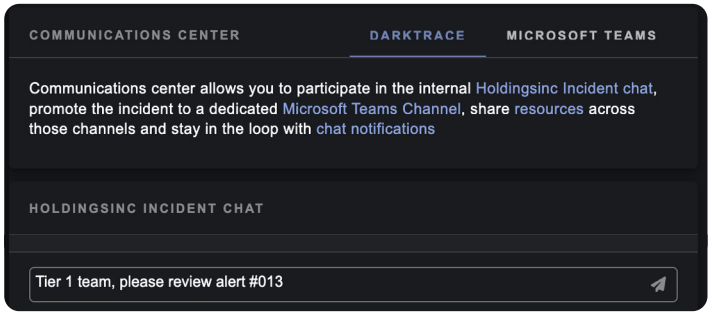
Remove handover and familiarization time between tools and services with an integrated incident interface that shows all the necessary information for seamless recovery.

This includes event details, containment actions, the highest risks that could happen next and recommended next steps. Integrations with EDRs, ticketing systems and popular data recovery tools ensure Darktrace represents the full scope of your IR processes.

This includes a streamlined communication centre that ensures greater team collaboration during stressful incidents.

Relevant business and security stakeholders can be informed, without responders taking their eyes off the threat. This channel shortens downtime as appropriate tasks can be delegated as soon the incident emerges.





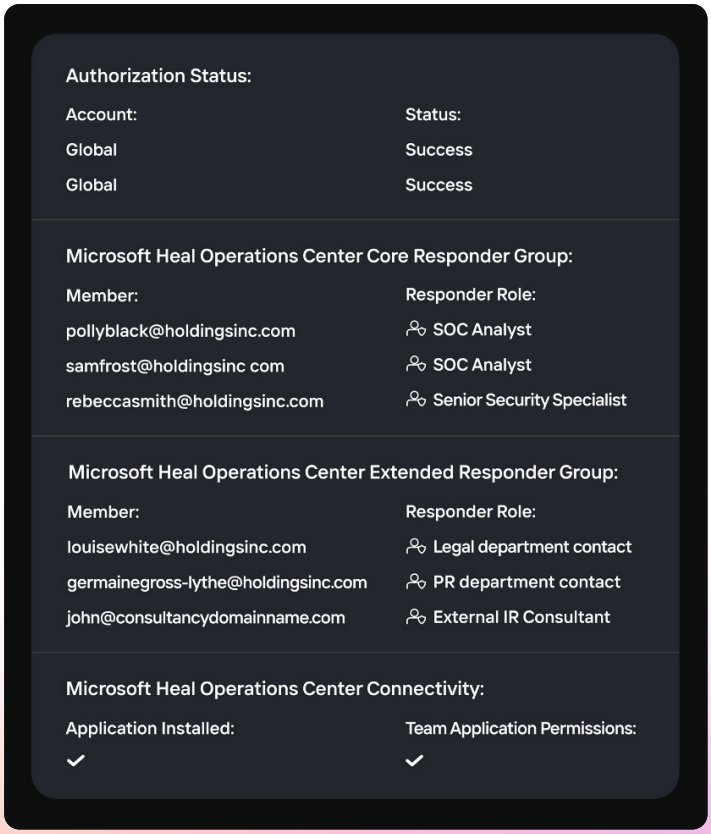
Reduce lengthy deliberation and feedback

Use Darktrace's existing understanding of **you** to establish: **how ready are you for a cyber-attack?**

With continuous evaluation, organizations gain a clear understanding of their cyber resilience and how to improve their risk posture most effectively.

Readiness Reporting shows the status of your technology and responder preparations so teams can be confident that everything will work when they need it to.

Incident Reports save time with an automated summary of completed and in-progress attacks, while Playbook reports support auditing functions. These can all be kept as a record, improve review cycles, or be used to inform third party stakeholders such as forensics or compliance authorities.



Deployment

Darktrace / Incident Readiness & Recovery permissions are granted on top of an existing Darktrace on-prem or virtual cloud master deployment.

Purpose-built integrations are available across various data back-up, mobile device management, communications and endpoint detection and response solutions. For more information check the Darktrace website.

Deployment steps

01	Ensure existing Darktrace / NETWORK deployment with call-home preferable
02	Darktrace support team will grant additional permissions for Darktrace / Incident Readiness & Recovery
03	Review underlying 'Recovery steps' that are used to make AI generated playbooks
04	Configure available API integrations if necessary
05	Schedule, run and engage your first simulation using one of the (Demo) templates

Operational benefits

Be prepared for anything
Cyber AI Analyst generates earlier detection, improved prioritization and tailored playbook creation with reduced decision-making time

Get the right people in the room
Ensure early delegation and transparent, undistracted communications with business and security stakeholders alike

Build resilience following an Incident
Closer monitoring and safeguarding by Darktrace detection and autonomous response for assets recently involved in an incident

Make the most out of your team
Incident simulations ensure IR processes are continually reviewed and assessed so teams are working at their best standard

Darktrace Platform & Portfolio

Resilience & the Darktrace ActiveAI Security Platform

Darktrace builds security solutions by looking at where AI can have the most positive impact on human security efforts. Darktrace / Incident Readiness & Recovery brings that philosophy to resilience by training teams and reducing the decision-making SOCs face during an attack, so they can recover and get back to business more effectively.

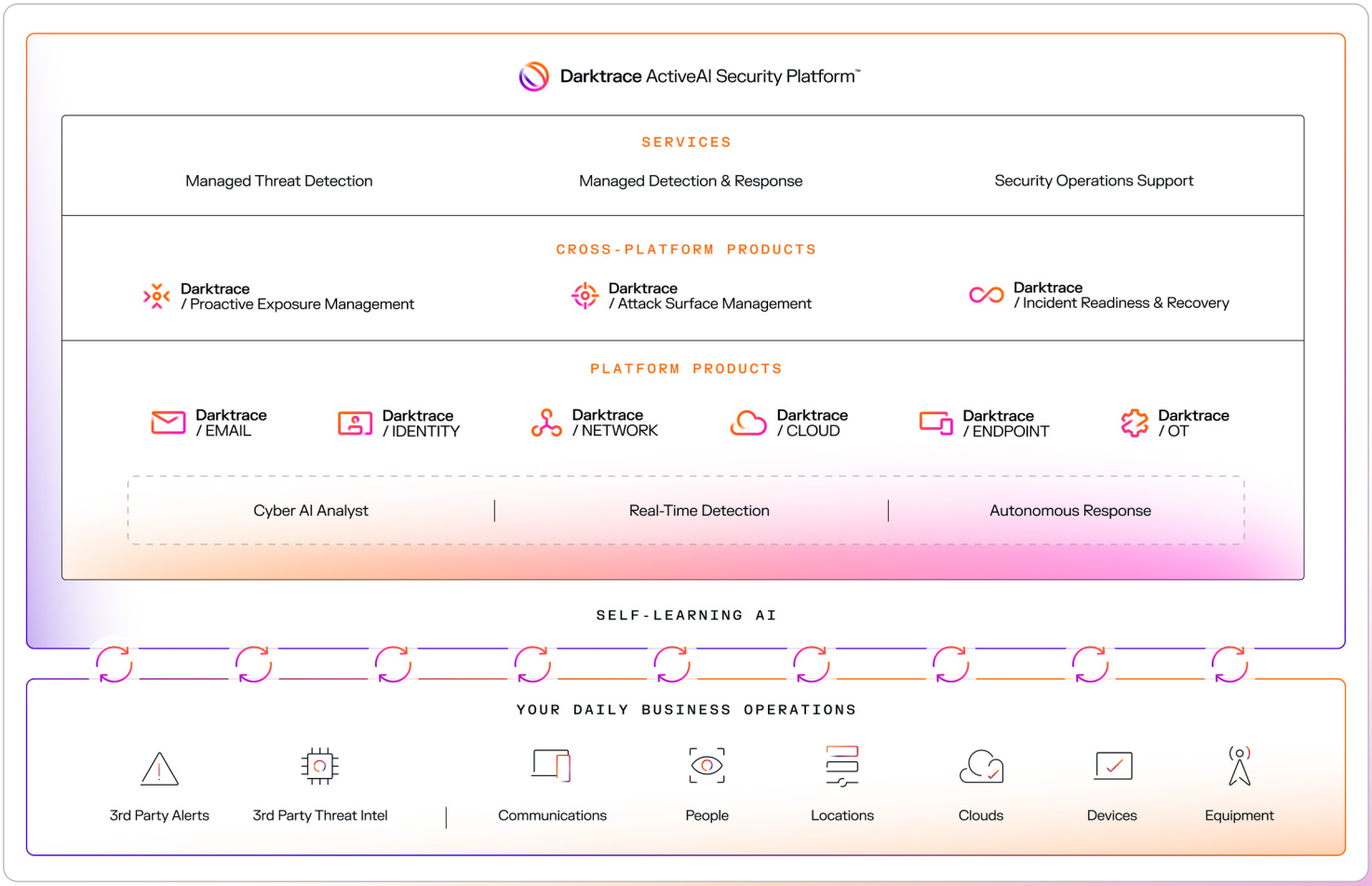
> Darktrace / Incident Readiness & Recovery not only returns our systems to a trusted operational state, but also hardens the system so that it is **stronger than it was before**.
>
> ■ CISO
> City of Las Vegas

Darktrace / Incident Readiness & Recovery takes information from across all components of a customer's Darktrace deployment to ensure recovery and adaptation following a compromise.

Together, in the context of the Darktrace ActiveAI Security Platform, Incident Readiness & Recovery ensures protection throughout the entire attack process, with organizations being able to anticipate, detect, contain, recover and learn from any cyber incident – which are core components necessary for cyber resilience.

Darktrace is the first of its kind to provide proactive cyber defense in a single holistic platform. To achieve this, Darktrace pioneered the use of ActiveAI Security that continuously learns from your day-to-day business operations, applying context from your enterprise data ingested from internal native sources including email, cloud, operational technology, endpoints, identity, applications and networks, and external sources of third-party security tools and threat intelligence.

Through this approach, Darktrace provides the ability to visualize and correlate security incidents uninhibited by the siloed approach of individual point.



About Darktrace

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a 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 help transform security operations and improve cyber resilience. Breakthrough innovations from its R&D Centers have resulted in more than 200 patent applications filed. Darktrace employs 2,400 people around the world and protects over 9,700 organizations globally from known, unknown and novel cyber-threats.

North America: +1 (415) 229 9100 Europe: +44 (0) 1223 394 100 Asia-Pacific: +65 6804 5010 Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com