# DARKTRACE DETECT™

AT A GLANCE:

- Bespoke – A deep knowledge of your enterprise and what constitutes a threat
- Real-time view – Always-on detection and analysis of potential attacks
- Full coverage – Operates across cloud, apps, email, endpoints, network, and OT
- Intuitive – Delivers simple outputs for security teams

## / Self-Learning AI that understands YOU

Where other cyber security solutions are trained to identify threats based on historical attack data and techniques, Darktrace DETECT takes a fundamentally different approach by seeking to deeply understand your organization and its 'normal' state.

It gains a bespoke understanding of your digital environment, continuously analyzing your users, assets, devices and the complex relationships between them.

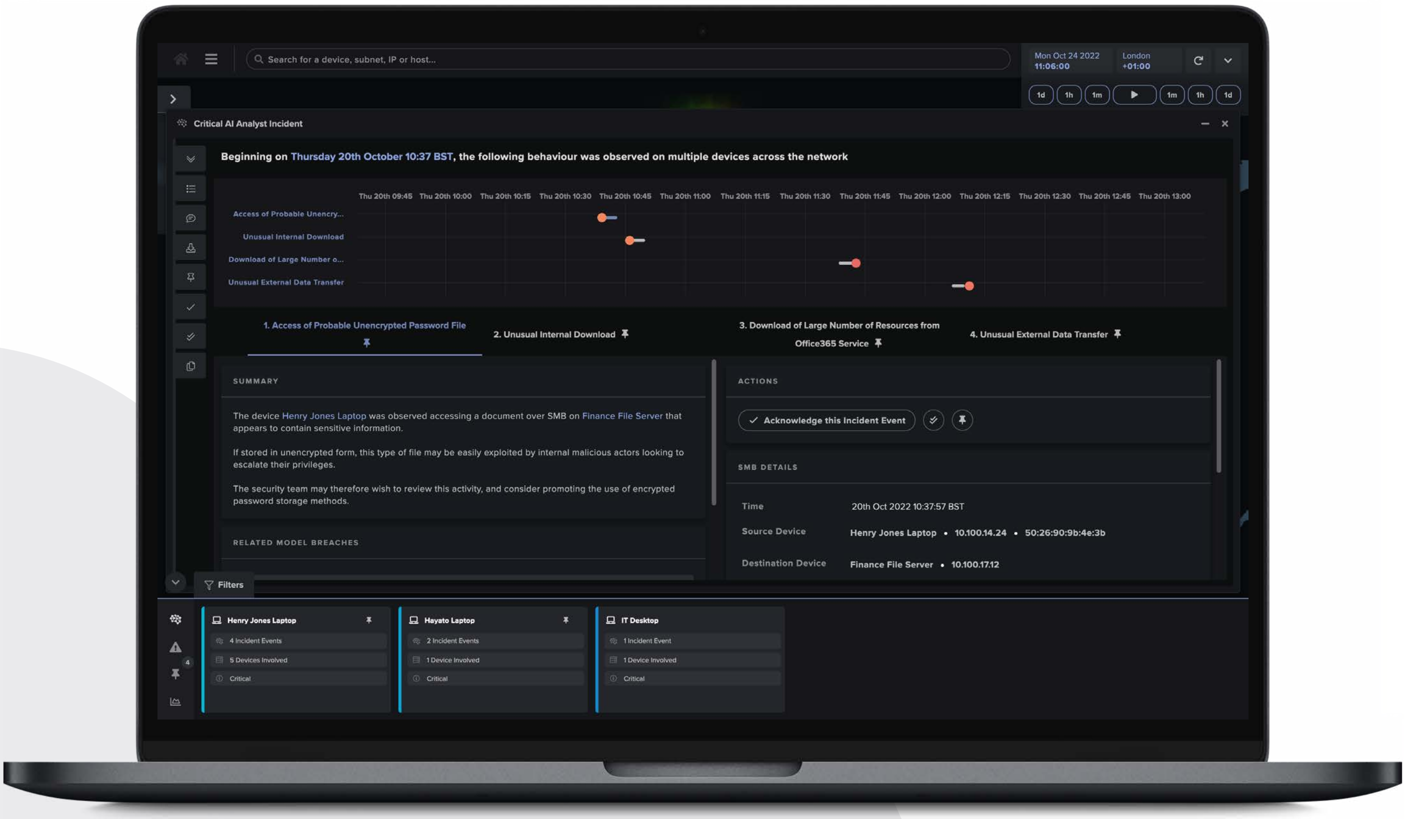
Through learning the everyday dynamics of your organization, Darktrace DETECT can identify the subtle deviations from normal activity that indicate emerging and never-before-seen threats – learning normal to identify abnormal.

> "Darktrace's AI algorithms are focused on one thing, and it's your organization."
>
> / CIO, Healthcare

## / Reduce time to triage by over 90%

Cyber AI Analyst connects individual threats to investigate attacks at speed and scale. It produces incident reports on critical events and the context around them, replacing the analysis that would normally fall to a human. By focusing on the highest priority threats, your security team can save valuable time and direct their expertise to the high-value work that humans do best.

> "AI Analyst is sophisticated and the intelligence it gives us is clear and actionable – even my newest and most inexperienced starters can use and learn from it on day one."
>
> / CISO, IT Management


Search for a device, subnet, IP or host...
Mon Oct 24 2022 11:06:00
London +01:00
1d
1h
1m
1m
1h
1d
Critical AI Analyst Incident
Thu 20th 09:45
Thu 20th 10:00
Thu 20th 10:15
Thu 20th 10:30
Thu 20th 10:45
Thu 20th 11:00
Thu 20th 11:15
Thu 20th 11:30
Thu 20th 11:45
Thu 20th 12:00
Thu 20th 12:15
Thu 20th 12:30
Thu 20th 12:45
Thu 20th 13:00
Access of Probable Unencry...
Unusual Internal Download
Download of Large Number o...
Unusual External Data Transfer
1. Access of Probable Unencrypted Password File
2. Unusual Internal Download
3. Download of Large Number of Resources from Office365 Service
4. Unusual External Data Transfer
ACTIONS
Acknowledge this Incident Event
RELATED MODEL BREACHES
Filters
4

Beginning on Thursday 20th October 10:37 BST, the following behaviour was observed on multiple devices across the network

SUMMARY

The device Henry Jones Laptop was observed accessing a document over SMB on Finance File Server that appears to contain sensitive information.

If stored in unencrypted form, this type of file may be easily exploited by internal malicious actors looking to escalate their privileges.

The security team may therefore wish to review this activity, and consider promoting the use of encrypted password storage methods.

SMB DETAILS

| | |
|---|---|
| Time | 20th Oct 2022 10:37:57 BST |
| Source Device | Henry Jones Laptop • 10.100.14.24 • 50:26:90:9b:4e:3b |
| Destination Device | Finance File Server • 10.100.17.12 |

| Henry Jones Laptop | Hayato Laptop | IT Desktop |
|---|---|---|
| 4 Incident Events | 2 Incident Events | 1 Incident Event |
| 5 Devices Involved | 1 Device Involved | 1 Device Involved |
| Critical | Critical | Critical |

Figure 1: Cyber AI Analyst displaying an incident report

## / Protection across your organization

Darktrace brings its AI to your data, wherever it is. It works across the entire digital ecosystem of your organization to track the full scope of every incident – from email, network and cloud applications to endpoint devices and Operational Technology (OT) – leaving attackers with nowhere to hide.

Cloud Apps Email Endpoint Network Zero Trust OT

While effective in any one of these single coverage areas, the Self-Learning AI becomes even more powerful when it is able to connect the dots across the entirety of your digital estate.

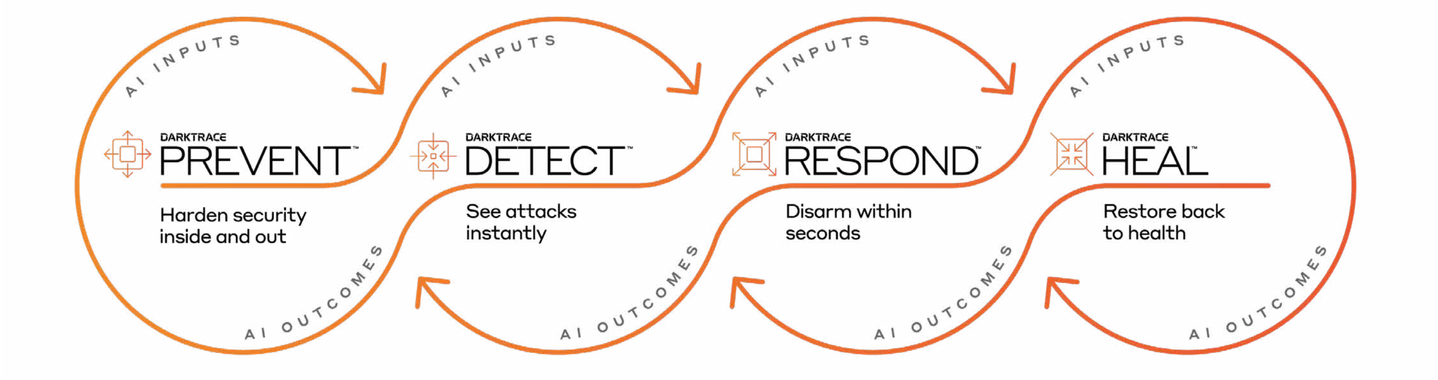
When deployed fully, DETECT can track potential attacks as they move across different coverage areas – such as an employee attempting to download sensitive files from multiple sources and transferring them outside of the company.

## / Quick set up; effective within days

Whether deployed in a specific coverage area or across your entire organization, Darktrace DETECT is quick and easy to set up – installing in minutes and learning the normal pattern of life for your enterprise from within a week.

Because DETECT learns 'on the job', it continues to adapt to your organization as it grows and changes – offering long-term protection against novel threats in an evolving threat landscape.

## / Cyber AI Loop



Darktrace DETECT forms part of Darktrace's technology vision of a Cyber AI Loop, which continuously optimizes and strengthens an organization's security at every stage of the attack life cycle – from proactive measures taken to harden security before an attack gets in, to detecting and responding to an attack.

Like all Darktrace technologies, DETECT becomes stronger when it is brought into the wider ecosystem of the Cyber AI Loop. The continuous feedback loop consists of four AI engines constantly feeding back into the system as a whole, maintaining cyber stability for an organization. For example, before an attack is launched, PREVENT is pre-empting and prioritizing possible entry-points and attack paths, highlighting risky and vulnerable assets to DETECT, with RESPOND then on high alert should anything suspicious happen to assets along these likely attack paths. Equally, DETECT analysis and RESPOND actions are fed back into PREVENT, which can then prepare for an attacker's next move.