Darktrace: Best Practices for Small Teams

Key Benefits

- ✔ Learns normal 'on the job' to detect unknown and unpredictable threats
- ✔ Neutralizes attacks at machine speed and with surgical precision
- ✔ Automates threat investigations at speed and scale, reducing triage time by up to 92%
- ✔ Offers unified and adaptive coverage of your entire workforce and business

Figure 1: Darktrace autonomously detects and responds to threats with surgical precision, 24/7

The Challenges of Protecting the Dynamic Workforce

Today's dynamic workforce is dispersed, agile, and unpredictable. In parallel, modern businesses are relying on increasingly diverse technologies, from cloud and SaaS services, to advanced IoT. And just as businesses evolve, so too does the threat landscape: security teams constantly face novel and advanced attacks, often moving at machine speed and hitting parts of the digital ecosystem that they are not prepared to secure.

At the same time, security teams are facing a staffing and skills shortage, and must manage disparate security stacks that more often than not present too many alerts to triage appropriately – leaving the real threats unnoticed or improperly managed.

Darktrace Immune System: Empowering Small Security Teams

The Darktrace Immune System allows even the smallest security teams to protect their dynamic workforces from the most sophisticated threats, while enhancing the value of existing investments through shared intelligence and active integrations.

Darktrace's Cyber AI never sleeps – meaning your team can trust that there is always an intelligent solution autonomously detecting, investigating, and responding in real time to threats as they emerge, without the need for configuration or constant tuning.

Instead, Darktrace learns the unique 'patterns of life' of your business and spots even the most subtle deviations from normal behavior that point to an attack – from advanced threats like **Dharma ransomware**, to zero-day nation-state attacks like **APT41**. The technology does not rely on rules or signatures, but rather uses unsupervised machine learning and advanced Bayesian mathematics to identify nuanced changes in activity.

Two core capabilities of the self-learning technology, Cyber AI Analyst and Enhanced Monitoring models, are designed to be reviewed within minutes. For teams that only wish to check the Darktrace Immune System interface briefly every day, these provide the platform's most vital benefits: the ability to instantly understand a situation and take immediate action when things are burning, where response time is of the essence.

Autonomous Investigations: How Cyber AI Analyst Augments the Human

For teams that only have five minutes a day to use Darktrace, the most critical capability to leverage is Cyber AI Analyst, which allows you to see immediately the most significant threats happening in real time. Cyber AI Analyst autonomously investigates every threat detected and highlights the highest-priority incidents at any one time – ensuring you see what needs attention right away.

The technology pulls together related events into a clear Incident Report, including an AI-generated natural language summary and a visual timeline of the threat. Security responders are able to grasp the severity of the incident immediately - ensuring severe threats like ransomware, data exfiltration, and a malicious insider attack are able to be actioned in minutes.

Incident Reports include a clear graphic pointing to where the threat sits in the kill chain. If there are several phases, it's likely a big attack and will need close, immediate attention. Security teams can easily skim through the related devices, subnets, scanning ports, sources, and the relevant details, which are all pulled into one place in the report. Cyber AI Analyst makes it easy to take just a few minutes to examine an incident and decide how to follow up.

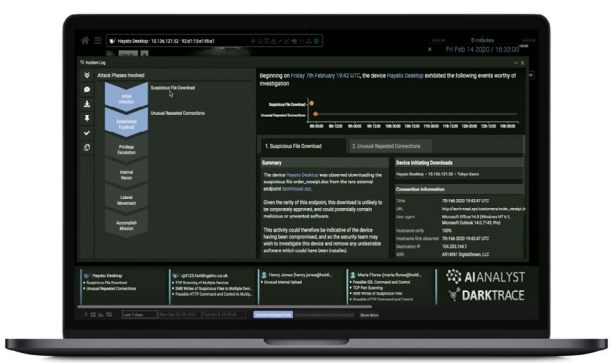

Figure 2: Cyber AI Analyst Incident Report with attack phases shown

On-demand Investigations

While Incident Reports are always created for the most critical threats at any one time, investigations can be applied on demand to suspicious devices or users by simply selecting the time window, the device or user of interest, and then clicking the 'Investigate' button within the Threat Visualizer. 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.

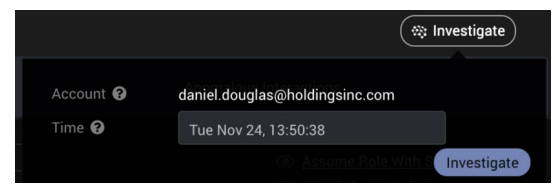

Figure 3: Easily trigger on-demand AI-driven investigations

Seamless Interoperability

Cyber AI Analyst technology can also be integrated with tools across your 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 your existing workflows.

> "With AI Analyst on demand, I have the flexibility to target my investigations. You can be more proactive, autonomously."
>
> Scott Rheins, IT Security Architect, Cardenas Markets LLC

Cyber AI Analyst Incident Tray

The Cyber AI Analyst incident tray is accessible from the 'Neural Network' icon in the bottom left of the threat tray within the Threat Visualizer. Incidents are categorized from blue to white, where white indicates the highest level of threat. Each incident will list the associated device, the derived device type, and a short summary of the events involved.

Cyber AI Analyst will always prioritize the most severe incidents in the tray for the specified time period. As it refines its understanding of each incident, incidents may reduce in severity or be replaced by emerging threats. The ‘Show More Incidents’ button can be used to retrieve incidents that you were previously investigating or wish to revisit, but are no longer highest in severity.

The Acknowledged/Unacknowledged filter shows or hides Acknowledged incidents. Incidents can be acknowledged on an event-by-event basis, in their entirety in the Threat Visualizer, or in the Mobile App. Acknowledging a Cyber AI Analyst incident does not acknowledge the underlying model breaches.

Any pinned Cyber AI Analyst incidents will always appear in the left-hand side of the incident tray. Click the 'Download Incidents' button to download a PDF report containing all current incidents in the tray.

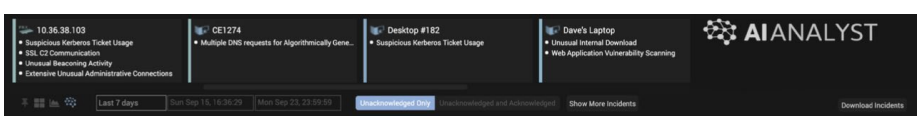

Figure 4: The Incident Tray shows the most significant incidents at any one time

> “With Cyber AI Analyst we can see the whole picture. It’s all right there in one place, with all the context and details we’d need to take action.”
>
> Rick Bertoncin, Director of Technology & Security, Gallagher-Kaiser Corporation

Incident Timeline

Click on an incident in the tray to launch the Cyber AI Analyst pane. An incident is composed of one or more events: events are a group of detected actions (model breaches) investigated by Cyber AI Analyst that pose a likely cyber-threat. At the top of the page is a clear timeline representative of the incident. Detections that are associated with each event will appear as dots, where color indicates severity.

The activity associated with an event currently selected from the tabs below the timeline will be highlighted in blue. Long-lived events, such as large data transfers, may cover a large chronological period. Antigena's Autonomous Response activity is also shown in green on this timeline.

Like a human, Cyber AI Analyst uses an initial detection of unusual behavior as a starting point for investigations. The behavioral analysis it performs may discover patterns of activity that were not the original trigger point for the detection but are worthy of investigation.

Consequently, the event period may not correspond with the model breach time. Additionally, some model breaches require sustained behaviors such as repeated connections before breaching, so the final breach trigger may be later than the connection of interest.

Figure 5: Each Incident Report shows a clear visual timeline of all the events involved

Incident Events

Each event will appear as a tab. The right panels will break down key elements of the event and the involved devices; the data is specific to each event type. The left panel gives a summary of the event.

Detections that triggered a Cyber AI Analyst investigation will be listed as related model breaches. Currently active or expired Antigena responses will be listed below the related breaches.

The action section allows for the individual event to be pinned, acknowledged, or acknowledged alongside all related model breaches.

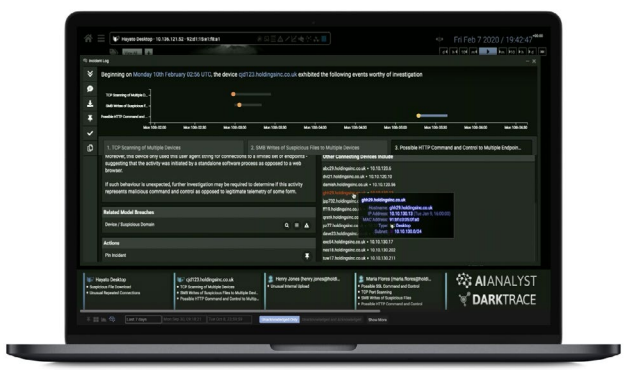

Figure 6: Incident Report showing related unusual behavior and connected device information

Attack Phases

Clicking the downward arrows on the left side of the pane will open a visual representation of attack phases involved in the incident. This view immediately indicates the scope and severity of the incident.

Download the Report

The 'Download' icon on the left offers the ability to easily download and share a PDF version of the Cyber AI Analyst Incident Report.

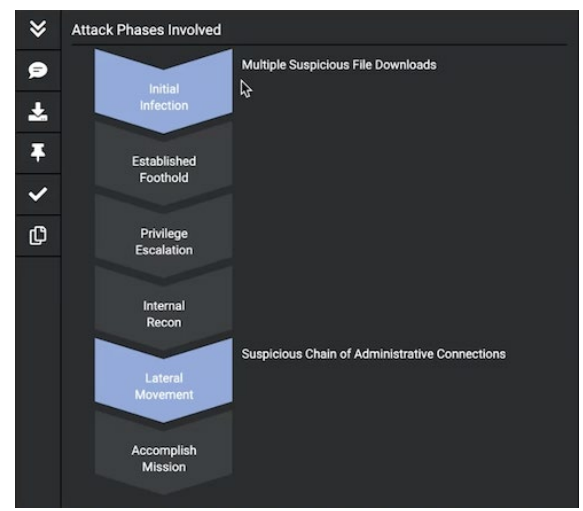

Figure 7: Each Incident Report includes a graphic highlighting attack phases touched

"The AI Analyst is sophisticated, but the intelligence it gives us is clear and actionable."

Mark Herridge, CISO, Calligo

Enhanced Monitoring: Highlighting 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.

Enhanced Model detections are available via the Threat Visualizer by selecting Threat Tray Filters and choosing Enhanced Monitoring. When Cyber AI detects a threat related to an Enhanced Monitoring model, you can get automatic email alerts for additional real-time notification.

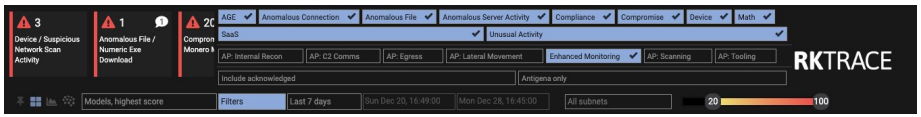

Figure 8: Filter for Enhanced Monitoring to see the most critical behavior detected

> "It's autonomous – AI Analyst and Antigena just work as expected for high-risk incidents, and we let it do its thing."
>
> Syed Hussaini, Cyber Security Analyst, Metricon Technology Group

Autonomous Response: The Machine Fights Back

Darktrace Antigena provides 24/7 Autonomous Response, neutralizing threats as they emerge – giving understaffed and overworked teams the critical time necessary to catch up.

For small teams, the first step on the journey towards truly autonomous defense is setting up Antigena to match your business needs. To that end, Antigena can easily be configured according to a range of flexible parameters:

- Degree of Automation: Configure Antigena to be fully autonomous or to require human approval before taking action
- Use Cases: Tailor Antigena to cover specific business risks, from insider threats to external attacks
- Timing: Schedule distinct Antigena parameters for different times of the week, including over the weekends or during business hours
- Scope: Consider where and to what extent Antigena actions should apply, whether globally or per subnet, user, device, or threat model
- Integration: Deploy Antigena to interface with third-party firewalls or network devices as a mechanism for response

Powered by self-learning Cyber AI, Antigena is the first and only solution that can interrupt attacks at machine speed and with surgical precision, even if the threat is targeted or entirely unknown. Every second, Darktrace Antigena stops an emerging cyber-attack – making it a critical tool for small teams to ensure workforces and workloads are always protected.

Cyber AI on the Go: The Darktrace Mobile App

The Darktrace Mobile App lets you protect your dynamic workforce and monitor your entire digital infrastructure on the go. Get real-time threat notifications, investigate the most significant incidents with Cyber AI Analyst, and control Antigena's Autonomous Response actions – all from your phone.

Self-defending Cyber AI gives you enterprise-wide coverage that evolves and grows with your business, and with our Mobile App you 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 incidents** that you find significant or email to a colleague
- **View and adjust** Antigena's Autonomous Response actions

"With the Darktrace Mobile App, my team can instantly respond to in-progress threats and authorize Darktrace's AI to fight back on our behalf – even outside of business hours."

Chris Zeller, Director of Information Security, Country Life Vitamins

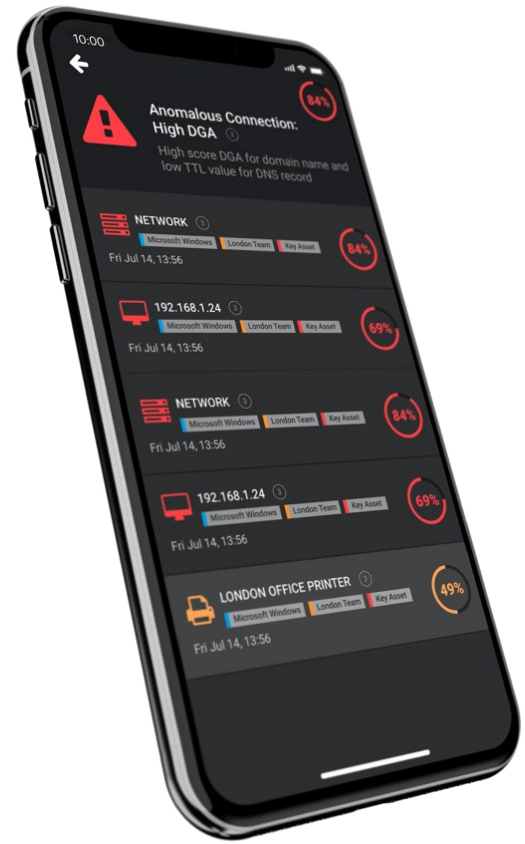

Figure 9: The Darktrace Mobile App lets you monitor your entire digital infrastructure on the go

Easy Win Integrations

The Darktrace platform was designed with an open and extensible architecture that seamlessly integrates with your 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 you don't see your chosen provider in 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's 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:** Extending Enpoint Protection

  Darktrace can ingest EDR alerts as weak indicators that inform our 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 & Zero Trust Technologies:** Defending the Dynamic Workforce

  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. Current customers can see the integrations guide **here**.

- **Single Sign On:** Seamless Access

  For ease of use, Darktrace natively supports authentication and access via SAML 2.0 Single Sign On. Current customers can see the integrations guide **here**.

"One-click integrations help our team identify the things we need to see, connecting the dots, making those correlations, and then making those alerts actionable for us. There's huge value in that for us."

Austen Ewald, Network Analyst, St. Charles Community Unit School District

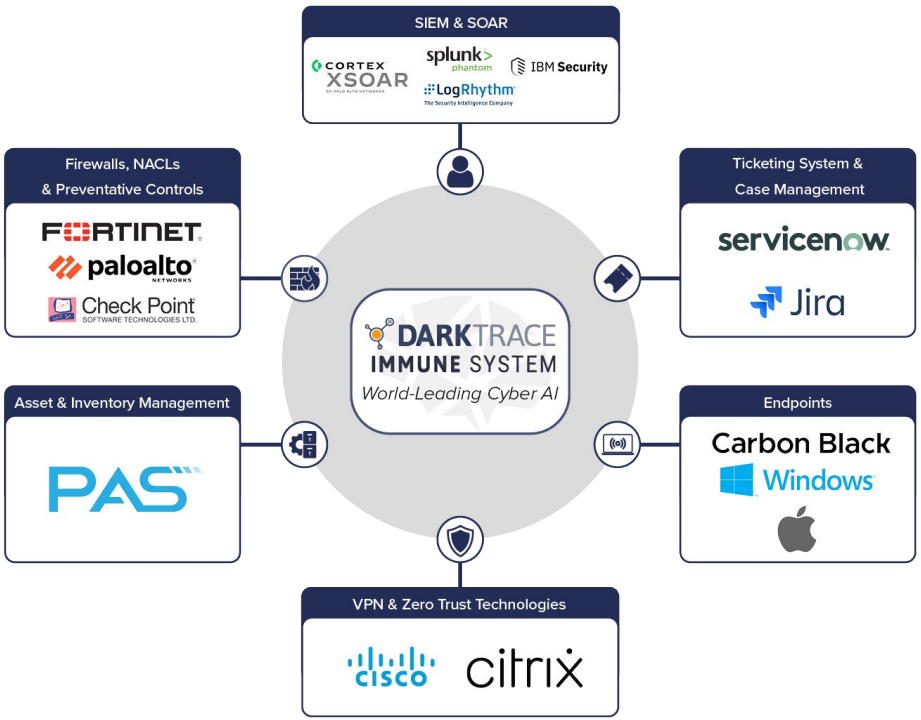

Figure 10: The Darktrace Immune System integrates seamlessly across the security stack, improving productivity and ROI

"Tying the Immune System into all these various integration points has unlocked so much potential in our SOC."

Ethan H., Security Engineer, A&M

Watch the Video: Maturing Your Use of Darktrace for Small Teams ›

About Darktrace

Darktrace is a leading autonomous cyber security AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,700 organizations to protect against threats to the cloud, email, SaaS, traditional networks, IoT devices, endpoints, and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every second, Darktrace AI fights back against a cyber-threat, before it can cause damage.

For More Information

- Visit darktrace.com
- Book a free trial
- Visit our YouTube channel
- Follow us on Twitter
- Follow us on LinkedIn