Darktrace Discoveries in Australia

How Cyber AI Defends Organisations from Attack

Navigating the Australian Cyber Landscape

Rapid changes in working patterns and digital infrastructure have led to significant developments in the cyber-threat landscape. In late 2020, some of the world's most trusted organisations – including branches of the Australian government – were targeted by nation-state actors. As the boundaries of corporate infrastructure become increasingly blurred and Australia continues to implement new regulations and strategies, businesses are turning to self-learning AI technology to autonomously fight back against threats.

> "Darktrace's ability to neutralize both stealthy threats and machine-speed attacks is nothing short of revolutionary."
>
> CEO, City Tattersalls Club

> "Darktrace has enabled us to take our cyber security to a level we presumed unattainable."
>
> Head of IT, Jackson McDonald

According to the Centre for Strategic and International Studies (CSIS), Australia stands as the 6th most targeted country in the world for cyber-crime. Sophisticated threat actors have ramped up their campaigns against Australian companies, and organisations across all industries from manufacturers to food production companies have recently fallen victim to major cyber-attacks.

Recognising the gravity of this threat, the Australian government announced the Cyber Enhanced Situational Awareness and Response (CESAR) package in June 2020, promising $1.35 billion over the next decade for cyber security, which includes creating 500 new cyber expertise jobs and bolstering the Australian Signals Directive (ASD) to repel offshore cyber-crime.

Two months later, Prime Minister Scott Morrison revealed Australia's new Cyber Security Strategy. This aims to support businesses and the community through consultations and best procedure guidelines, promoting complementary action between "governments, businesses, and the community". The government is investing $62 million to train organisations on how to deal with attacks and working with large businesses to support SMEs which cannot afford an extensive cyber security team.

Today, Australian companies are under pressure to comply with a range of cyber regulations. From the financial sector's APRA CPG 234 requirements to the energy sector's AEMO framework, public and private bodies are pushing to achieve higher levels of cyber maturity across their diverse IT, OT, and IoT ecosystems.

The Department of Home Affairs (DHA) have made clear that organisations in all sectors can be held accountable if they fail to implement adequate security measures. Companies across Australia have been encouraged to adopt an adaptive approach to defence, one that keeps up with advancing threats and evolves alongside changing, complex digital ecosystems.

Consequently, hundreds of Australian organisations have turned to Darktrace Cyber AI to help defend their infrastructure from attack and to safeguard their critical systems and data. By learning 'on the job' and creating a bespoke understanding of the digital DNA of each organisation and its people, Darktrace is uniquely able to stop threats which bypass the majority of signature-based tools.

"Businesses should take responsibility for enhancing their cyber security, just as they are responsible for the safety and quality of their products."

Australia's Cyber Security Strategy 2020

Threats by Numbers

- Every 10 minutes the Australian Cyber Security Centre (ACSC) reports a cyber-attack
- $29 billion total annual cost of cyber-attacks for Australian companies
- 59,806 cyber-crime reports received by the ACSC from June 2019 – June 2020
- $30 billion (1.5% of GDP) and 163,000 lost jobs predicted if a cyber-attack were to disrupt digital infrastructure for one month

"Darktrace thrives in complex digital environments as the technology is adaptive, enabling it to detect and respond to threats that other tools miss."

Research Director, IDC

Darktrace Immune System

Autonomous Cyber Security Across the Enterprise

Relied upon by Australia's leading organisations across multiple sectors, Darktrace's Cyber AI detects and responds to cyber-threats seconds after they emerge. Like the human immune system, the self-learning AI develops an understanding of 'normal' for each user and device in an organisation, and all the connections between them, continuously revising this understanding in light of new evidence and fighting back against malicious activity.

Darktrace's Immune System platform consists of three tightly-integrated, AI-native systems: the Enterprise Immune System, which leverages unsupervised machine learning to detect threats in their earliest stages, Cyber AI Analyst, which automates threat investigation and reporting at the speed and scale of AI, and Darktrace Antigena, Autonomous Response technology which surgically responds within seconds to neutralise cyber-attacks.

"Darktrace not only augments our security team in detecting subtle anomalies but is used extensively across IT functions and is openly discussed by our C-Suite."

Information Security Manager, Grant Thornton Australia

Darktrace evolves alongside your business, including through times of unprecedented change. The AI analyses diverse systems and distributed users to autonomously detect, investigate, and respond to attacks across all environments, from email, cloud, and SaaS platforms, to endpoints, IoT, and the corporate network.

The Darktrace Immune System was designed to seamlessly integrate with cloud services and zero trust environments, as well as existing security investments such as firewalls and SIEMs.

Figure 1: Darktrace Antigena autonomously responds to cyber-threats in seconds

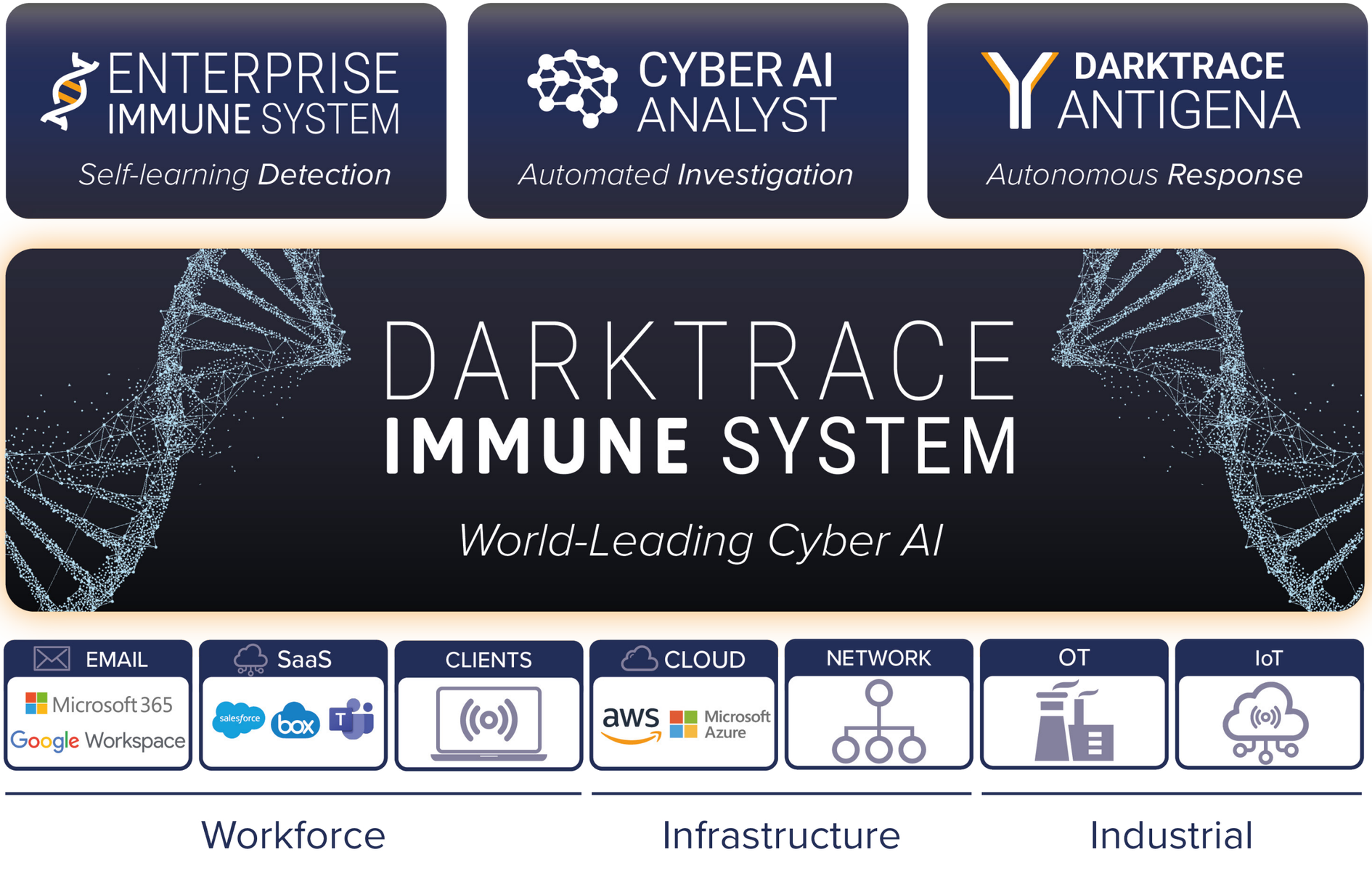


Figure 2: Darktrace's Immune System platform

Case Studies: Protecting Australian Customers

Detecting Unauthorised Password Access at The Y NSW

The Y NSW is one of the oldest and biggest youth organisations in the world, with a small team managing its entire digital infrastructure. The company regularly has large numbers of employees and volunteers connecting to its system, and yet it lacked the oversight to be able to understand what was happening within the digital ecosystem.

The Y deployed Darktrace Cyber AI for a 30-day free Proof of Value (POV) trial. After one hour, Darktrace established a 'pattern of life' by learning the activity of its dispersed workforce.

An insidious threat arose when a file containing passwords was accessed by an unauthorised user on the network. Darktrace immediately detected the threat and alerted the charity's IT team, allowing them to identify the user and remediate the issue immediately – a threat which would have gone unnoticed otherwise.

"We could immediately understand how Darktrace would improve our security posture from day one and how valuable the technology would be. No other tool can detect threats as fast."

Head of Information Technology, The Y NSW

In 2020, when The Y was forced to close its physical facilities and conduct its operations digitally, Darktrace aided its transition and remotely defended its business. With the Darktrace Mobile App, the charity's security team remain connected to its IT infrastructure at all times and can respond to threats as soon as they occur. Darktrace's Mobile App enables access to the Threat Visualizer and allows the team to benefit from unparalleled threat detection and complete visibility of the remote workforce.

Figure 3: Darktrace's Threat Visualizer graphically displays events of interest and provides full visibility across the business

Australian Cyber Landscape

Autonomous Cyber Security

Case Studies

Threat Finds

Optimising Girton Grammar School's Lean Security Team

Girton Grammar School is an independent co-educational school located in Central Victoria and is one of Australia's oldest schools. Each year, the school provides 350 junior school students with laptops and desktop computers that they can use in school and allows 750 senior school students to bring their own devices. Even before the school shifted to teaching lessons online, defending these devices in home environments was of high importance for the team.

With an IT team of just four people, the school turned to Cyber AI to protect students' data. While the team used to typically 'spend hours digging from scratch' in order to identify possible threats, this is now made easy with the Enterprise Immune System autonomously detecting anomalous behaviour and categorising threats according to severity. Darktrace empowers the IT team to decide whether or not to immediately address and resolve a given issue and enables them to focus on high-level tasks, allowing the AI to do the heavy lifting.

During the COVID-19 pandemic, Darktrace adapted alongside Girton Grammar School to defend its remote working environments. With Darktrace, the school remains connected to its IT infrastructure at all times.

> "Darktrace made everything so much easier, it radically simplified something that was incredibly complex."
>
> ITC Manager, Girton Grammar School

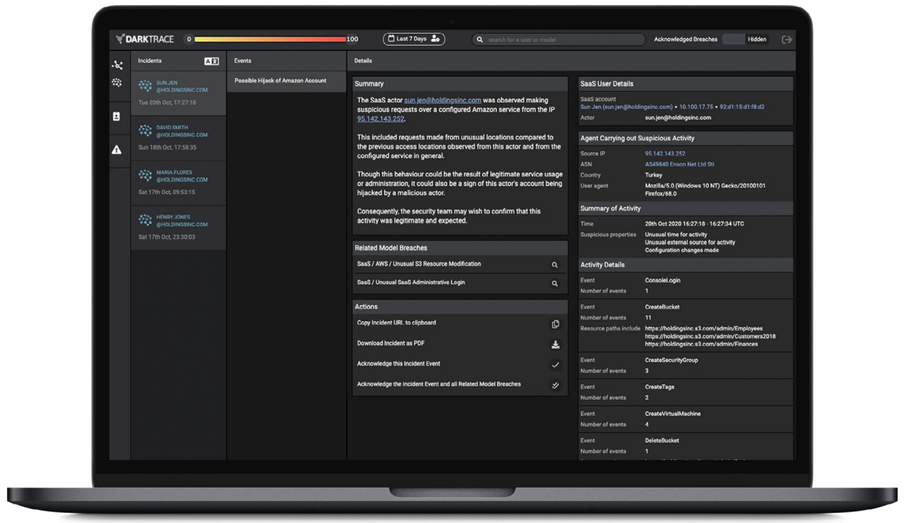


Figure 4: Darktrace's Enterprise Immune System detects threats across the entire digital ecosystem, no matter where or when they emerge

Threat Finds: Self-Learning AI in Action

Mimecast Miss Leads to Widescale Compromise

An Australian logistics company had Mimecast operating in their Microsoft 365 environment. When the company decided to trial Antigena Email, Darktrace's AI immediately detected that the company was under sustained attack from a cyber-criminal who had already performed account hijacks on a number of their trusted suppliers and partners. The attacker had sent out several tailored emails from these third-party accounts to the logistics company – threats that slipped through the gateway.

Antigena Email was being trialled in Passive Mode, so while the malicious email was identified and flagged, no proactive intervention took place. One of the Australian company's employees clicked on a malicious link contained in these hijacked emails which led them to a fake Microsoft login page for credential harvesting. Three hours later, an anomalous SaaS login was detected on the corporate account from an IP address not seen across the business before. Shortly afterwards, Darktrace detected an anonymous sharing link being created for a password file.

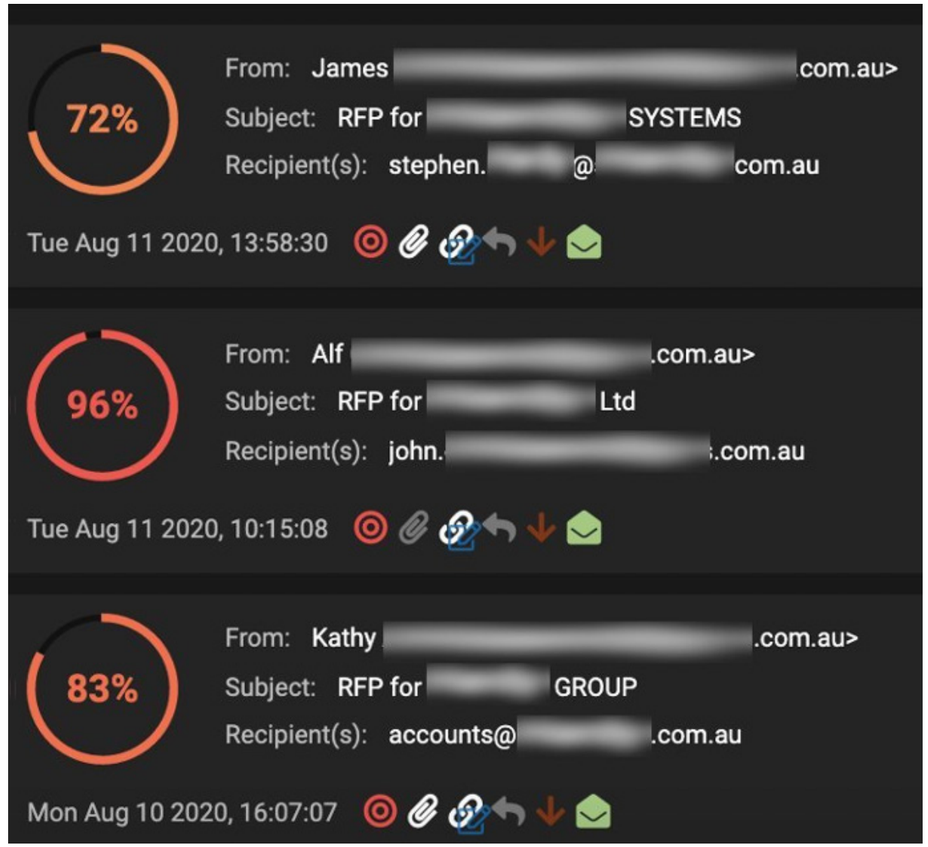
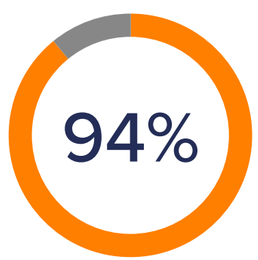


Figure 5: A sample of the malicious emails from the hijacked accounts; the red icon indicating that Antigena Email would have held these emails back



of cyber-attacks start with an email

The following day, the attacker sent out further malicious emails from this account to trusted business associates using the same methodology as before – sending fake and targeted RFPs in an attempt to compromise credentials.

Darktrace's SaaS module identified this anomalous behaviour, demonstrating on the interface how the attacker had sent more than 1,600 tailored emails over the course of 25 minutes.

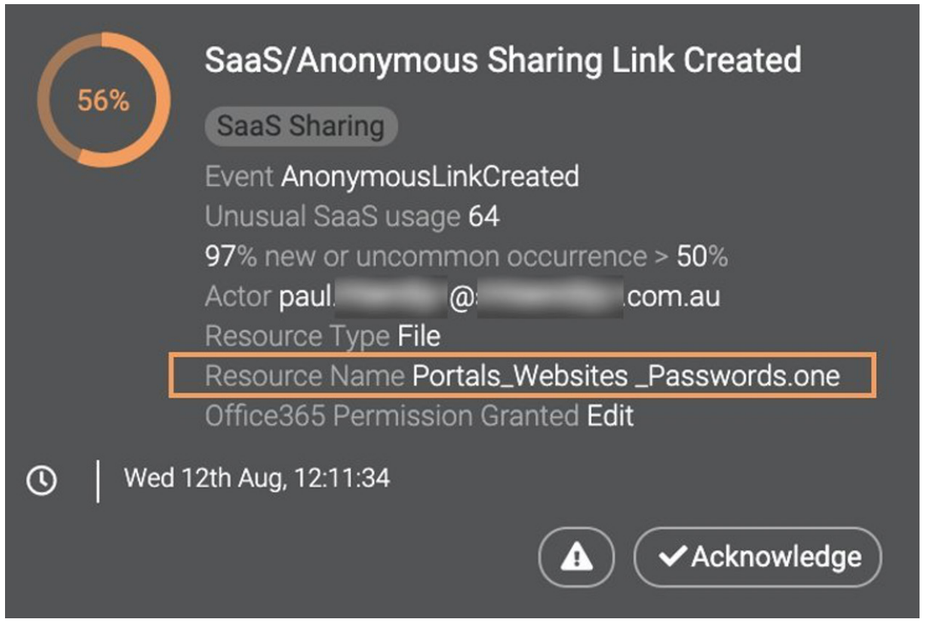


Figure 6: Darktrace's SaaS Module revealing the anomalous creation of a link

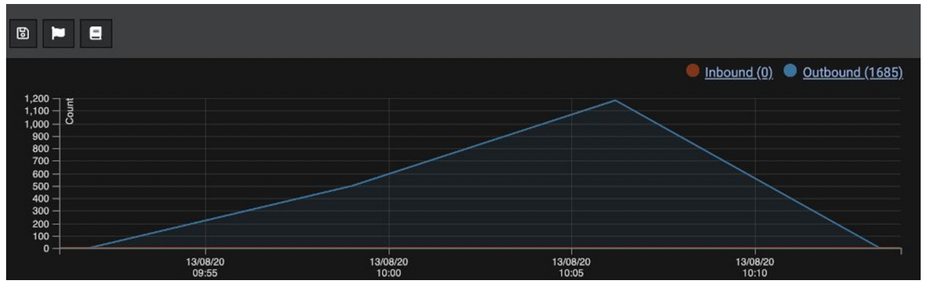


Figure 7: A graphical representation of the burst of emails sent over a 25-minute period

The Managed Security Service Provider (MSSP) running their cloud security was completely unaware of the account takeover. However, with Darktrace's SaaS module working alongside Antigena Email, Cyber AI gave the security team full visibility of the attacker's activity.

This incident caused the organisation to deploy Antigena Email in Active Mode, which now stops even the most subtle and targeted threats that attempt to enter through the inbox.

Australian Non-Profit Organisation Attacked via RDP Intrusion

In mid-2020, a large not-for-profit organisation begun trialling the Enterprise Immune System in their Melbourne-based headquarters. Shortly after being implemented, Darktrace detected several servers receiving remote desktop protocol (RDP) connections from suspicious endpoints based in unusual locations.

Concerningly, Darktrace observed the same servers making outbound RDP connections to these anomalous endpoints, suggesting that the servers were compromised by one or more attackers. Darktrace was able to provide confidence that the attacker had not yet begun exploiting their high level of access to the organisation's critical infrastructure.

When presented with the information, the organisation confirmed the activity to be unauthorised and begun steps to disable external RDP connections on the relevant servers. As a handful of these servers still required external RDP connections due to a legacy setup, the organisation opted to use Darktrace Antigena to autonomously prevent future unauthorised external connections, RDP or otherwise, from occurring.

Without Darktrace, the company could have been in serious trouble. After infecting an organisation through an internet-facing system like RDP, a threat actor can spread laterally and launch any number of attacks, including data exfiltration and ransomware. Below is a chronological overview of the Darktrace detections that fired during a separate attack on a customer without Antigena in Active Mode, which resulted in a full-scale Dharma ransomware infection. The Darktrace Immune System detected every stage of the attack, sending high-priority alerts to the security team in real time.

Sun Apr 12, 15:03:04	win-n981rj30565.	.local breached model	Compliance / Incoming Remote Desktop
Sun Apr 12, 13:45:06	win-n981rj30565.	.local breached model	Anomalous File / Internal / Additional Extension Appended to SMB File
Sun Apr 12, 13:45:05	win-n981rj30565.	.local breached model	Compromise / Ransomware / Ransom or Offensive Words Written to SMB
Sun Apr 12, 13:45:04	win-n981rj30565	.local breached model	Compromise / Ransomware / Suspicious SMB Activity
Sun Apr 12, 13:43:05	win-n981rj30565	.local breached model	Compliance / Incoming Remote Desktop
Sat Apr 11, 17:57:45	win-n981rj30565.	.local breached model	Compliance / Incoming Remote Desktop
Sat Apr 11, 15:28:01	win-n981rj30565	.local breached model	Compliance / Incoming Remote Desktop
Fri Apr 10, 12:46:56	win-n981rj30565	.local breached model	Compliance / Incoming Remote Desktop
Fri Apr 10, 11:40:06	win-n981rj30565.	.local breached model	Compliance / Incoming Remote Desktop
Wed Apr 8, 12:49:03	win-n981rj30565	.local breached model	Device / Anomalous RDP Followed By Multiple Model Breaches
Wed Apr 8, 12:49:03	win-n981rj30565.	.local breached model	Device / Anomalous SMB Followed By Multiple Model Breaches
Wed Apr 8, 12:49:02	win-n981rj30565.	.local breached model	Device / Large Number of Connections to New Endpoints
Wed Apr 8, 10:10:34	win-n981rj30565.	.local breached model	Anomalous Connection / Application Protocol on Uncommon Port
Tue Apr 7, 12:29:16	win-n981rj30565	.local breached model	Compliance / Internet Facing RDP Server

Figure 8: An overview of Darktrace detections during a Dharma ransomware attack; the initial point of entry was an RDP server

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 demo
- Read our blog
- Follow us on Twitter
- Follow us on LinkedIn