Darktrace backs Biden strategy as market cap nears $10bn

Cambridge-based cyber security world leader Darktrace saw its market cap soar closer to the magic £7 billion landmark today – making it arguably one of the most valuable tech businesses Cambridge has ever produced. It equates to not far short of $10bn in US currency.

The share price was up 16p to 966p this morning (Friday) on the back of even more good news: Darktrace revealed that its Self-Learning AI is defending organisations across all 16 critical infrastructure sectors designated by the Cybersecurity and Infrastructure Security Agency (CISA).

Within CISA, the Office of Infrastructure Protection leads efforts to manage risks to critical infrastructure, deeming them "essential to the economy, security, and sustainment of the American way of life."

Self-Learning AI has proved crucial in this mission. It augments human teams and takes autonomous action to detect and respond to threats against the country's most sensitive systems and critical data – at the earliest stages of an attack.

Self-Learning AI works by constantly evolving its understanding of both IT and operational technologies, allowing it to identify the subtle, emerging signs of a cyber-threat and take targeted action to interrupt encroaching attacks. These real-time alerts enable critical infrastructure organisations to continue business operations without disruption.

The technology also allows defenders of critical

infrastructure to achieve the Biden Administration's goals outlined in the National Security Memorandum on Protecting Critical Infrastructure Control Systems – namely threat visibility, indications, detections, warnings, and facilitating response.

Darktrace Self-Learning AI has successfully fought back against insider threats, supply chain attacks, zero-day exploits, APTs as well as state-sponsored attacks across US critical infrastructure industries.

In May 2021, hackers hit Colonial Pipeline with ransomware, forcing the company to halt the pipeline's total operations to contain the attack. In the same month, Darktrace AI detected, investigated, and contained a double extortion ransomware attack on a water and wastewater organisation in North America.

Unlike in the case of Colonial Pipeline, the attack was interrupted before hackers could demand any ransom payment or disrupt business operations. Darktrace catches ransomware and other security threats similar to this every day across all 16 sectors.

"The Florida water system attack was a huge wake-up call for us. If hackers get access to credentials, they could leverage them to gain entry to enterprise systems then laterally move to the operational system," said Bryon Black, IT manager at South Coast Water District in Laguna Beach, California.

"Darktrace's Self-Learning AI has provided our team with enhanced visibility into our entire digital environment and how our staff operate. Autonomous Response allows Darktrace AI to take action and mitigate risks as threats arise – helping to prevent the spread of lateral movement."

Marcus Fowler, director of strategic threat at Darktrace added: "Despite the Biden Administration's aspirations for critical infrastructure to be 'off-limits' from hackers, these

organisations remain the top target from nation-states and cyber-criminal groups alike.

“The reality is, whether motivated by espionage or financial gain, or simply seeking to cause disruption, attackers are already within some of our critical systems.

“Self-Learning AI is vital for defenders of critical infrastructure, allowing them to spot the breadcrumbs of attacks before they escalate, interrupt them autonomously, and minimise disruption – keeping data, employees, and citizens safe in a new era of cyber-attacks.”

• PHOTOGRAPH: President Joe Biden in the East Room of the White House. (Official White House Photo by Adam Schultz)