# The Emergence of Self-Learning, Self-Defending Cyber Security Solutions in a Landscape of Fast-evolving Threats

Darktrace, a world leader in Enterprise Immune System technology for cyber security, has won several awards, including the Queen's Award for Innovation in 2016. Its Enterprise Immune System technology automatically detects and responds to cyber threats without human intervention and before any damage can be done. By applying the Bayesian Estimation theory, mathematicians at the University of Cambridge developed this award-winning machine learning software.

Mr. Sanjay Aurora is the Managing Director of Darktrace Asia Pacific, where he has led in its expansion in the region since 2015. With over 25 years of experience in the enterprise software industry in the Asia-Pacific region, Sanjay is an influential figure in the field of emerging cyber security solutions.

Mr. Sanjay Aurora
Managing Director,
Darktrace Asia Pacific

**HIMSS Asia Pacific speaks to Mr. Sanjay to learn more about the trends of cyber threats, especially those facing the healthcare industry, and how we can strengthen our defense against these threats.**

## Thank you for making time to speak with us, Mr. Sanjay. As an IT expert with over 25 years of experience, what are the biggest cyber threats facing healthcare organizations in Asia Pacific?

**SA:** The healthcare industry faces some of the most pressing cyber security challenges, due to the **proliferation of connected devices, extreme sensitivity of the data, and often leaner security teams.** As a result, healthcare providers have remained a top target globally for sophisticated threat-actors. Darktrace's Enterprise Immune System self-learns what 'normal' is for every user and device on the network and uses that baseline to spot threatening anomalies as they emerge.

## How does the system inform organizations that deploy it of what is happening? What role do healthcare IT professionals within these organization play vis-à-vis this intelligent auto-defense system?

**SA:** The Enterprise Immune System learns the 'pattern of life' of every device and user on the network and uses that understanding to detect threatening anomalies as they emerge. Security teams get a bird-eye view of the earliest signs of an attack and can remediate emerging threats before they have escalated into a crisis. **To date, Darktrace's AI technology has detected over 30,000 serious in-progress threats.**

We have now taken the next step and leveraged this tried-and-tested technology to take appropriate, measured remedial action. This automated response is a true manifestation of AI in cyber – The Enterprise Immune System is the first and only AI technology that can do this. The machine can now fight back, augmenting human teams by buying them precious time to catch up in an increasingly automated cyber arms race.

## Does the 'immune system' learn perpetually?

**SA:** Yes, the Enterprise Immune System continues to learn and deepen its understanding of an organisation's 'normal' pattern of activity by applying the machine learning and AI algorithms developed at the University of Cambridge. **These unique AI algorithms continue to learn outside the laboratory of their creators, able to detect threats in real-world, dynamic environments.** Just like a human security professional, the technology recalibrates its understanding in light of new facts and models an understanding of 'normal' for that network which constantly evolves with the organization. In this way, Darktrace's self-learning technology can detect 'unknown unknowns' missed by legacy tools reliant on rules and signatures.

## Our current protection mechanisms still revolve around the signature, walls, rules-based and locks-based system. How can healthcare organizations be encouraged, or educated, to move towards machine learning technology?

**SA:** We will continue to see more serious attacks on the healthcare sector until organizations realize that they are at risk and adopt machine learning to protect their data, systems, and critically, their patients. Healthcare organizations need to ask themselves, **'what would happen if X piece of equipment got hit with ransomware today?', or 'how would we know if an attacker were to change one patient's data, and how would we remediate the situation without bringing all operations to a standstill or putting lives at risk?'.**

Cyber security is now a cyber arms race. Humans can no longer keep up with the speed and sophistication of modern threats. This calls for technology that does more than sit at the border and stop pre-identified threats from jumping the fence, but AI systems that detect the early indicators of fast-evolving threats already on the network.