Wellcome Trust

Overview

Industry
• Non-profit

Challenge
• Sensitive intellectual property to protect
• Healthcare data an attractive target for cyber criminals
• Gain complete visibility of the network

Benefits
• Real-time visibility and investigation of the network
• Self-learning approach
• Next-generation detection of emerging anomalies

Business Background

Founded in 1936 by entrepreneur, collector and philanthropist Sir Henry Wellcome, the Wellcome Trust is an independent global charitable foundation dedicated to improving health. Science and research expand knowledge by testing and investigating ideas, and this new understanding can be applied to health and change medicine, behavior and society.

The Wellcome Trust supports thousands of curious, passionate people all over the world to explore great ideas, from discovery to impact, giving focused, intensive support when it sees real opportunities to transform lives. The Trust has an unyielding commitment to improving human health through science and research, drawing on 80 years of achievement to adapt as new ideas and challenges arise.

The Trust holds an £18 billion investment portfolio which provides the income for its funding. It intends to spend up to £5 billion over the five years leading up to 2020.

Challenge

With the increasing digitization of healthcare records and medical processes, and the fact that medical records can be sold for up to 20 times the price of a stolen credit card number, the industry has become a major target for cyber attackers.

As well as financial and privacy concerns, there exists the more serious possibility of medical data and research being unknowingly changed. Even minor changes to a patient’s blood type or list of known conditions could clearly put entire healthcare systems into a state of chaos and destroy their integrity and ability to operate.

The Wellcome Trust was aware that in the context of today’s cyber-threat landscape, its critical systems and networks were vulnerable to new, evolving cyber-attacks from all over the world.
This was a matter of concern for the company and it wanted to gain a better understanding of its network in order to proactively monitor emerging threats.

Solution
In response to its complex security needs, Wellcome Trust chose to deploy Darktrace’s Enterprise Immune System. The Enterprise Immune System is based on unsupervised machine learning and Bayesian mathematics developed at the University of Cambridge. Established with the insight of government intelligence officers, it is a self-learning cyber-threat platform that begins to gain a sense of ‘self’ in a network as soon as it is installed. With this probabilistic understanding of what is abnormal to a network, it allows Wellcome Trust to remain confident that potential cyber threats will be detected before they cause damage.

With Darktrace’s unique ability to detect abnormal behavior as soon as it occurs, Wellcome Trust could optimize its capacity for effective threat mitigation. Simultaneously, the company finally had a comprehensive picture of its entire network, with full visibility into every digital behavior and exchange.

Benefits
Darktrace’s Enterprise Immune System offers Wellcome Trust the means to stay ahead of emerging threat actors that jeopardize the entire sector, with the ability to adapt to the changing information environments that the healthcare system relies on, and to detect abnormal behaviors in real-time.

Thanks to the Enterprise Immune System’s ability to learn a sense of ‘self’ within an organization, Wellcome Trust now has unprecedented awareness of its entire network. This visibility allows for an understanding of all anomalies, not just those immediately deemed to be threatening. The ability of the Enterprise Immune System to determine the estimated threat level of each particular anomaly, and to bring the most immediately worrying to the attention of security personnel through the Threat Visualizer, means that Wellcome Trust can stay ahead of even novel forms of attack. Darktrace’s software is therefore uniquely proactive in the way it protects Wellcome Trust’s information, as well as the trust’s long-term brand reputation.

The Trust has gained an invaluable defense capability through full network visibility to take control of its digital infrastructure and make decisions based on real-time developments, allowing it to remain proactive in the face of even the most advanced forms of cyber-threat.