DARK TRACE

Irwin Mitchell

IM irwinmitchell solicitors

Overview

Industry

○ Legal

Challenge

○ Protect against potential threats, including APTs

○ Safeguard client data and confidentiality

○ Stay ahead of an evolving threat landscape

Results

○ Detection of anomalies within the network, which were previously unknown

○ Total network visibility

○ Increased confidence in the security and integrity of client data

○ Ability to investigate incidents in real time and 'replay' them

○ Ability to take control of evolving situations, rather than react

Business Background

Established in 1912, Irwin Mitchell is amongst the 20 largest law firms in the UK, with 11 offices across the country. With over 2,400 employees, Irwin Mitchell is a 'full service' law firm and delivers a wide range of private client and business legal services to private individuals, businesses, charities, institutions and organizations. Winner of numerous industry awards, Irwin Mitchell is a leader in its sector, with a reputation for excellence and innovation.

> "
> Darktrace allows us to show that we are on top of cyber security: we are monitoring, we are alerting, we are investigating, and not just small areas of our network but all of our network.
> "
>
> **Mark Vivian**
> **Head of IT Security**

Challenge

Irwin Mitchell has long prioritized the integrity of its data systems, and particularly that of its clients' information. In particular, the firm wanted to improve its ability to detect potential cyber-threats, or suspicious incidents, early, by acquiring a better understanding of the activity of its networks and where, if anywhere, unexpected events might be occurring.

Ultimately, Irwin Mitchell wanted to have the confidence that if something abnormal was happening in their systems, it would be able to deal with those situations before they escalate, and tangibly mitigate risk.

Solution

Following a thorough assessment of the cyber security market, Irwin Mitchell decided to trial Darktrace's Enterprise Immune System technology. "When I first saw the product, I was skeptical if it could actually deliver, because it was so different," says Mark Vivian, Head of IT Security at Irwin Mitchell. "After my discussions with Darktrace and having seen the demo, I decided to see what it could do, which is why we went for the Proof of Value."

"The installation and the configuration literally took about half an hour," said Mark Vivian. Within a couple of weeks, Darktrace had learned enough about the firm's network to be able to deliver extremely insightful information about its network and users.

Based on unsupervised machine learning and probabilistic mathematics developed at the University of Cambridge, the Enterprise Immune System works by developing a 'pattern of life' for each user, device and organization, and can detect subtle deviations from what it understands to be 'normal' behaviors. Without any 'a priori' knowledge of specific threats or the data environment, the self-learning Enterprise Immune System automatically models an organization's activity, correlating its findings and continually refining its judgments.

"Once we started to see some of the results, we were reassured that our systems had not been compromised. But we did find a couple of configuration and process issues, which would not have been detected without Darktrace." The Proof of Value (POV) demonstrated that the Enterprise Immune System could deliver genuine value to the business, through its advanced detection, 100% network visualization and investigation capability.

> **"**
> The installation and the configuration literally took about half an hour.
> **"**
>
> **Mark Vivian**
> **Head of IT Security**

Benefits

"Cyber security is not a 'nice to have' anymore, it's a must have. And you've got to protect not only your client information but also your own. Having cyber insurance and ISO 27001:2013 is becoming a baseline of what is required, but it's not enough. Darktrace allows us to show that we are on top of cyber security: we are monitoring, we are alerting, we are investigating, and not just small areas of our network but all of our network."

Using Darktrace's Threat Visualizer, the investigation interface that provides 100% visibility of network activity, Irwin Mitchell uses Darktrace not only as a general intelligence tool for data integrity and protection, but also for a variety of functions from application support to root cause analysis.

The Threat Visualizer not only shows anomalies and incidents that are worthy of investigation, but also automatically classifies threats based on their seriousness. This enables the team to instantly focus on what is most important at any one time, amid the noise of a busy network. Darktrace also provides the ability to play back incidents, as well as play them in real time, in order to conduct in-depth investigations and understand the context of particular incidents.

"I think it's quite a big game changer for us to be able to not only see our network in real time, which is useful, but also to be able to go back in time and play it at any time," says Mark Vivian from Irwin Mitchell. "For me, it has been a massive benefit in understanding what's actually happening."

In the context of an increasingly sophisticated threat landscape, Irwin Mitchell uses the self-learning capability of the Enterprise Immune System to stay ahead of potentially-emerging problems, giving the firm and its clients greater confidence about the protection of its most critical assets. Ultimately, it lets Irwin Mitchell adopt a modern, proactive stance to security, however the network or threats might evolve.