EUROPEAN FINANCIAL SERVICES LEADER

Self-Learning Approach Delivers Next-Generation Cyber Defense

Overview

Industry

- Financial Services

Background

- Vulnerable to data loss and damage to data integrity
- Insider threat problem
- Needed to address targeted attacks with no historic precedence
- Protect information while retaining flexibility

Results

- Detected anomalies from day one
- Allowed action to be taken early in the attack cycle
- Adapts to evolving business environment
- Next-generation defence against advanced threats
- Addresses both external and insider threat

Business Background

This company is a leading mutually-owned financial services provider, with nearly 2 million members.

Challenge

The financial services sector not only faces the risk of data loss and leaks, but also the danger of their information and systems being unknowingly compromised, either by outsiders that have infiltrated their networks or by insiders.

Whilst traditional security tools focus on the boundaries of the network, it has become clear that it is not possible, practical or desirable to 'lock up' information systems from pervasive risks. This company wanted to be able to take action against advanced threats and potential issues from within their organization, before they escalate to become more challenging problems.

Solution

This leading building society decided to employ Darktrace's unique Enterprise Immune System technology to address the combined challenge of external and internal threats. Darktrace Cyber Intelligence Platform, powered by ground-breaking Bayesian probabilistic mathematics developed at the University of Cambridge, is the only solution capable of detecting unusual behaviors in real time, without any a priori knowledge of what it is looking for. DCIP's self-learning ability means that it is constantly refining its probability calculations, based on the evidence that it sees from the organization, at the level of each device, user and the network as a whole.

This company uses Darktrace's world-leading 3D threat visualization tool as well, the Threat Visualizer, to allow it to instantly respond to in-progress threats. The Threat Visualizer allows the company's analysts to better understand what is happening within their information systems and focus on mitigating the most important risks that are evolving in real time.

Emerging anomolies
were detected in
real time, which had
bypassed all other cyber
security tools.

Benefits

Within weeks of implementing Darktrace, this financial services leader was alerted to a number of anomalies that were unknown to their security team and unseen by its existing security tools.

Firstly, Darktrace detected indications of a potential reconnaissance mission, the early stage of an attack when an attacker looks around its target environment for vulnerabilities. Password guessing was taking place on a secure link and this activity was flagged as anomalous, according to Darktrace's dynamic understanding of the organization.

Darktrace also spotted a set of user credentials trying to authenticate into devices across the network over a 24-hour period, as well as one machine that was conducting port-scanning. Both these events were judged to be highly irregular by DCIP too, and therefore were exposed in the Threat Visualizer in real time as potential anomalous issues.

The customer was able to immediately investigate these early indicators of in-progress attacks, giving them the benefit of time, understanding and Darktrace's unique specialist expertise in order to mitigate against mounting risk and curb their damaging missions.

ABOUT DARKTRACE

Darktrace is the world's fastest-growing cyber defense company and the leader in Enterprise Immune System technology, a new category of cyber solutions based on pioneering Bayesian mathematics developed at the University of Cambridge. Darktrace addresses the challenge of insider threat and advanced cyber-attacks through its unique ability to detect previously unidentified threats in real time, as manifested in the emerging behaviors of the network, devices and individuals. Some of the world's largest organizations rely on Darktrace's adaptive, self-learning platform to spot anomalous activity within the enterprise, in sectors including energy and utilities, financial services, telecommunications, retail and transportation. Darktrace was founded by world-class machine learning specialists and operational government intelligence experts. The company is headquartered in Cambridge, UK, with offices in London, Milan, New York, Paris, San Francisco and Washington D.C.

CONTACT US

US: +1 (917) 363 0822
Europe: +44 (0) 1223 350 653

Email: info@darktrace.com

www.darktrace.com