DARKTRACE

CASE STUDY

CordenPharma

Overview

Industry

- Healthcare

Challenge

- Safeguarding business-critical intellectual property
- Lack of visibility over internal activity and third-party suppliers
- Difficulty detecting and thwarting targeted cyber-attacks
- Responding to fast-acting threats with lean security team

Results

- Deployed the Enterprise Immune System and Darktrace Antigena
- Achieved 100% visibility across the entire digital infrastructure
- Darktrace Cyber AI Platform became an essential force multiplier
- Gained ability to proactively respond to threats at machine speed

Business Background

CordenPharma manufactures pharmaceuticals for many of the world's leading pharmacies and biotechnology firms. Over the last several decades, the multinational company has contributed significant advances to Active Pharmaceutical Ingredient (API) manufacturing. Tasked with protecting critical intellectual property in the face of machine-speed cyber-threats, CordenPharma's security team knew it could no longer rely on the tactics and tools of the past.

> With the automated attacks we're up against, we can't afford to conduct a full investigation before taking action. That's where Autonomous Response has been indispensable: it puts the time factor back on our side.
>
> **CordenPharma**

Challenge

Many of CordenPharma's customers are in early-stage clinical drug trials and thus require strong data protection. It takes several years and billions of dollars to bring new pharmaceuticals to market, a process which requires the safe-keeping of both patient information and confidential IP. As a consequence, the pharmaceutical industry continues to be targeted by sophisticated cyber-attacks. In particular, threat-actors often attempt to compromise major pharmaceutical providers by first breaching their supply chains — composed of third parties who often have access to sensitive data outside the security team's purview.

Given its lean security team, CordenPharma also needed a technology to augment its manpower. Legacy tools — rooted in fixed 'rules and signatures' — flag any activity that meets broadly defined technical parameters, often inundating teams with a flood of false positive alerts. Not only do such alerts generate an inordinate amount of unnecessary labor, they also lead to genuine threats becoming buried and even overlooked entirely.

Solution

Following a four-week Proof of Value (POV), CordenPharma decided to deploy the Darktrace Enterprise Immune System and Darktrace Antigena across its expansive digital infrastructure. The Darktrace Cyber AI Platform leverages advanced AI algorithms to distinguish between normal and abnormal activity for each individual user and device, learning their typical 'patterns of life' while on the job. Thus, unlike conventional security tools that apply the same rules across the board, Darktrace's understanding of CordenPharma's unique business enables it to discern the subtly anomalous behavior indicative of a threat. And when such a threat requires urgent action, Darktrace Antigena — the first enterprise-grade Autonomous Response technology — contains it in seconds without interrupting normal operations.

> It was eye-opening to witness the capabilities we had with Darktrace. It lets our small security team of four look like we are a team of 20.
>
> **CordenPharma**

In fact, Antigena proved its value immediately during the trial period, when the company suffered a crypto-mining attack that was sapping a significant amount of computer power. Right away, the Enterprise Immune System discovered the behavior and determined it was abnormal for the firm, as the compromised device was beaconing to an endpoint in Hong Kong to which it had never connected before. Antigena would ordinarily have blocked this behavior, but it was deployed in 'Passive Mode' for the POV, meaning that it simply recommended its actions to the security team.

Because that team happened to be preoccupied, Antigena's 'Passive Mode' setting served to illuminate how the Autonomous Response technology works throughout a crypto-mining attack. After the anomalous beaconing activity, the device downloaded an executable from the Hong Kong endpoint, which Antigena would have again intervened to prevent. Eventually, an outbound data transfer of over 1 GB was initiated. At this point, Antigena would have stopped the device from transferring any data to the foreign endpoint. Antigena's ability to intelligently and surgically remediate the incident would have averted any damage, convincing CordenPharma to deploy Antigena in 'Active Mode'.

Benefits

Darktrace provides 100% visibility across CordenPharma's digital enterprise from a single interface, the Threat Visualizer. Moreover, the alerts that it displays are prioritized automatically, allowing the lean security team to rapidly triage security incidents. The Threat Visualizer is comprehensive: the security team can trace specific activity or users across time, replaying historical incidents at any level of detail.

One of the principal benefits of Darktrace's Cyber AI Platform is its ability to alert CordenPharma to threatening incidents early — before they can become damaging attacks. Such real-time intelligence affords both CordenPharma and its customers confidence in the security of their data.

Contact Us

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com