Palantir

IMPACT STUDY

COMBATING INTERNATIONAL CYBER ATTACKS

A large, multi-national corporation that provides services to numerous governments and industries was struggling to ensure the security of its complex computer network. Needing a way to protect its information resources from the growing threat of cyber attacks, the organization looked to Palantir for solutions.

THE PROBLEM

The organization faced the growing threat of cyber attacks from sophisticated adversaries. These adversaries operated in a landscape of data that was massive in scale and highly disparate. Armed only with conventional tools, investigators spent hundreds of hours analyzing data, yet they had trouble determining even basic elements of the attacks. The separation, diversity, and quantity of data made it difficult and time-consuming for analysts to leverage all the data and nearly impossible for investigation teams to collaborate effectively. As a result, the organization was caught off guard against its cyber adversaries, knowing neither when its systems had been infiltrated nor the degree to which the enterprise had been compromised.

PALANTIR'S SOLUTION

The Palantir Cyber solution, which includes Palantir's Phoenix technology for the integration and analysis of massive-scale data, provided the organization's analysts with a single point of access to billions of unique network events. After identifying relevant data, investigators could bring the data into the Palantir Workspace for rapid search and analysis in a unified environment. Each attack investigation was saved to the Palantir Revisioning Database, which implements a version control model that enables collaboration without risking data integrity. Senior analysts were able to collaborate easily across work locations and new analysts were able to get up to speed quickly because the organization's enterprise knowledgebase grew with every case. By using Palantir Cyber to stitch together insights from several analysts, the organization was able to gather vital intelligence on its adversaries and identify the infrastructure used by its cyber attackers.

PALANTIR'S IMPACT & RESULTS

» **Within the first hour** of investigation, geographically disconnected investigators were able to collaborate and **discover previously unknown information**.

» Investigators were able to **discover all computers affected** in a given attack and block traffic going out to the attackers' command and control servers.

» The organization was able to **transform from a cyber attack victim** trying to minimize losses into an organization **actively conducting counter-intelligence** against its adversaries.

FOR MORE INFORMATION

www.palantir.com