USE CASE Data Loss

Case Scenario

Andrea Danti/ShutterStock.com

Recently, Waymo an Alphabet (Google) company that is developing autonomous car development company, announced a $1.8 billion lawsuit against Otto and Uber, also in the autonomous vehicle business. According to Waymo, several former employees stole Waymo’s highly confidential and proprietary LiDAR design plans. The technology is critical to the development of autonomous cars—measuring the shape, speed and movement of objects like cyclists, vehicles and pedestrians.

Waymo’s investigation regarding the data theft states that “six weeks prior to resigning, Anthony Levandowski, a key Waymo employee at the time, downloaded over 14,000 highly confidential and proprietary design files for Waymo’s various hardware systems, Source code related to the self-driving car project, including designs of Waymo’s LiDAR and circuit board. To gain access to Waymo’s design server, Mr. Levandowski searched for and installed specialized software onto his company-issued laptop. Once inside, he downloaded 9.7 GB of Waymo’s highly confidential files and trade secrets, including blueprints, design files and testing documentation marked “Google Confidential and Proprietary”. Then he connected an external drive to the laptop and copied the files. Mr. Levandowski then wiped and reformatted the laptop in an attempt to erase forensic fingerprints. In addition to Mr. Levandowki's actions, Waymo reported that "other former Waymo employees, now at Otto and Uber, downloaded additional highly confidential information pertaining to our custom-built LiDAR including supplier lists, manufacturing details and statements of work with highly technical information."

Challenge

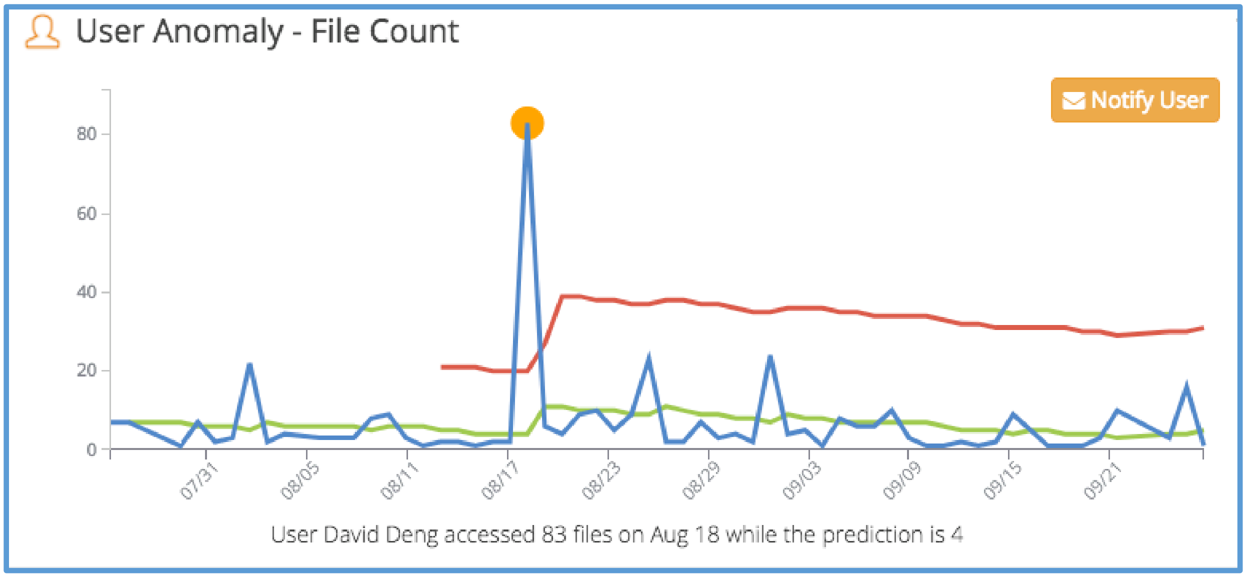
This unfortunate, high-profile incident is a classic example of the insider threat. As part of Google, the #44 ranking company on the Fortune 500 list, Waymo has vast resources at their disposal to secure their data. They have deployed multiple sophisticated security systems and yet they failed to detect the data breach in real time. The use of multiple security tools provides a partial and incomplete picture of your security. Individually they each perform their respective tasks well, but each supports a fragmented model for enterprise security. Using multiple, siloed technologies requires extensive configuration, long deployment times, and specialized security expertise to operate and analyze incident information. The result: undetected breaches, analyst fatigue, and inefficient investigations and remediation.

Solution

HoloNet OnFire™ functions like a real time surveillance and security "camera", but is focused on digital assets in cyberspace. Enabled by our patent-pending Network Hologram technology, OnFire automatically uncovers the hidden relationship among four security vectors – users, devices, applications, and data, and reconstructs the relationship in such a way that every moving digital asset, i.e., sensitive data, is linked to its actual user in real-time. Instead of going through weeks or months of manual procedures, security teams can simply "replay" and instantly see what has happened for any security incident investigation. With such precise correlation and user profiling, OnFire can provide accurate anomaly alerts and minimalize false positives.

By combining the best of UEBA, CASB and DLP technologies into a single powerful Data-centric Audit and Protection solution, HoloNet OnFire completely redefines what it means to protect an organization's most valuable asset: sensitive business data.. Had Waymo installed OnFire several months prior to the data breach, OnFire would have captured a precise user profile of Mr. Levandowski, including his typical user data volume as well as the devices and applications he accessed. When Mr. Levandowski started the data exfiltration, downloading thousands of files and multi-gigabytes of data within hours, OnFire would have detected the data anomaly as this behavior clearly exceeded the established baseline.

As shown in the following graph, the high watermark reached is clearly above and beyond the established baseline as represented by the green line. At this critical point, before any damage could be done, OnFire would have alerted Waymo's security team and prevented the incident.



User David Deng accessed 83 files on Aug 18 while the prediction is 4