securonix

CASE STUDY

Revealing Intellectual Property Loss in the Manufacturing Industry

CASE STUDY

Revealing Intellectual Property Loss in the Manufacturing Industry

Large Manufacturing Company

A Fortune 500 manufacturing company founded over 150 years ago and based in the United States. The organization currently employs 60,000 people with locations in more than 30 countries across the globe.

The Challenge: Detect Intellectual Property Theft

A manufacturing company needed to be able to detect intellectual property (IP) loss in order to lower the risk of confidential and proprietary information leaving the organization. All of their IP was housed in a custom application on PTC Windchill, which required security monitoring to detect and respond to IP theft.

The company formed an IP protection team to identify, classify, and detect IP loss. The IP protection team was responsible for identifying and classifying all data considered intellectual property in PTC Windchill. After that, in order to detect IP loss, the protection team needed to define access privileges for each IP classification and gain visibility into users accessing sensitive data, and then monitor for possible abnormal behavior signaling possible IP loss.

Key Challenges

- Require visibility into suspicious or abnormal access of sensitive data such as IP
- Lack of a security monitoring solution to detect data exfiltration
- Need the ability to manage user access rights and flag incidents to reduce the risk of data theft or data exfiltration

The Solution: Find Abnormal Behaviors Signaling Possible Data Theft

The manufacturing company chose Securonix to monitor their IP data and access privileges while also ensuring compliance mandates are met. Using Securonix UEBA the IP protection team was quickly able to learn what normal interactions look like, and then start investigating high-priority anomalous events involving IP files. Using behavioral analytics, Securonix detects sudden spikes in user access and flags them as anomalies. Then, the security team could investigate the activities to understand if they were caused by malicious actors or just those attempting to access sensitive information through their normal course of work.

The Business Impact: Detect and Respond to IP Loss

The IP protection team uses Securonix UEBA to spot abnormal user behaviors and activities in their environment. The security team once spotted an unclassified user trying to access a drawing file that they had never accessed before, which triggered an alert indicating a security violation. Upon further investigation, the team found that a datasheet with a hyperlink to a schematic of sensitive IP data had previously been shared with a partner organization. That datasheet was still connected to confidential intellectual property kept on an internal server and had not been updated in accordance with new security protocols. With Securonix, their security team was able to quickly identify the gap and fix the security protocol to reduce IP data loss.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.

For more information visit securonix.com