precisely

Customer Case Study:

International Airline Eliminates Mainframe Security Blind Spot with Ironstream for Splunk®

Challenge

A large international airline uses the Splunk Enterprise platform, along with the Splunk Enterprise Security app, to monitor its systems and applications in real-time for specific security scenarios, such as data leakage, unauthorized access and anomalous activity. However, this solution did not support the company's critical mainframe assets, causing a significant blind spot that put it at risk. They needed a log data feed for their User and Entity Behavior Analytics (UEBA) system to check for anomalies on the mainframe.

Solution

After evaluating potential solutions for getting mainframe logs into Splunk, the airline's Architecture Review Board selected Precisely's Ironstream for Splunk solution, based on its superior functionality and integration with Splunk, plus very low mainframe overhead compared with the competition. Ironstream captures the required mainframe records in real time and forwards them to Splunk with minimal impact on existing mainframe processing.

Results

With Ironstream's real-time capabilities, the airline has improved security and reduced risk. It now has enterprise-wide visibility, inclusive of its z/OS mainframe environment, and alerting for security issues as they happen . Ironstream also enables the airline to monitor mainframe availability through a log heartbeat.

For more information about Precisely's Ironstream for Splunk solution, visit: www.precisely.com