precisely

Case Study:

Healthcare Leader Turns to Ironstream for Splunk to meet SOC2 regulations

Challenge

Like so many other enterprises, one particular healthcare company was having trouble meeting all the varied requirements for certification under the standard known as SOC2. The SOC2 standard focuses on non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy. These standards also apply to the systems that touch the data.

SOC2 reporting requirements include the proper monitoring of log-on attempts, password changes, and user access violations. Given this system's size and growth — it manages a portfolio of diverse health-related businesses serving 50 million people — that's a lot of records to access and analyze. To process all the relevant SMF security records generated each day by its three IBM mainframes, the company was using IBM's zSecure products with some home-grown code. Not only was that approach too labor-intensive, but it didn't meet all their reporting requirements -- particularly those for the claims processing application running on their mainframes. It was clear they needed a better solution.

Solution

For some time, the company had been discussing the problem with Precisely as well as a number of other vendors in the SIEM (security information and event management) space. Their search for a solution kicked into high gear when they were facing important compliance targets that had to be met in just a few months time. Precisely quickly arranged a Proof of Concept (POC) demonstration of its Ironstream product together with Splunk Enterprise, using a sample of the customer's own SMF data.

The POC proved Ironstream's ability to replace the zSecure manual processes. That, plus the value-pricing and the track record of the Ironstream + Splunk Enterprise combination at other companies persuaded them to choose the solution over the competition.

The customer began securely forwarding ~20 gigabytes of SMF records per day through Ironstream to the Splunk platform for efficient, real-time monitoring and analysis – a volume that could eventually grow to 800 GB per day when you factor in growth and additional mainframe data sources. With Ironstream's innovative filtering, though, they can minimize the streamed data to include only those that are relevant to the use case.

Among the results

- The monitoring of security activity on their mainframe applications in Splunk Enterprise, including log-on attempts, password changes, user access violations, etc., met the audit and compliance thresholds for SOC2 certification
- The manual processes and related efforts and costs associated with using zSecure were eliminated
- The SMF forwarding became automated and started being done in real-time
- They were able to select and forward to Splunk Enterprise only those records related to security and compliance, without having to process the entire SMF record set, significantly reducing the volume of data forwarded and controlling resource consumption

With Ironstream's comprehensive file-type support, ease of use, low overhead, and innovative filtering, this healthcare leader can easily expand to other use cases while keeping costs to a minimum. They are equipped to garner new insights from their data and can easily adapt to changing needs.

To learn more about these types of ITOA-based improvements with the industry-leading Ironstream + Splunk Enterprise approach, visit: https://www.precisely.com