MEAS™

USE CASES

USE CASE #1: This client is a multi-billion dollar distributor and is a division of a global auto parts company. The client purchased MEAS in September of 2013. When they started evaluating SIEM technologies they had a requirement to support their 6000 MIPS (now 9000 MIPS) mainframe environment. However, none of the SIEM vendors had any mainframe expertise and tried to discount the need to support the zOS environment. The client tried to develop a tool on their own but did not have the internal resources available to dedicate to the effort. As a result, the client agreed to POC MEAS with their SIEM.

The client was able to satisfy their requirements within a few days. Their first priority was to monitor access to specific mainframe datasets by monitoring the datasets and the privileged users' access (system programmers and data base administrators). The client knew that privileged user credentials were and are still a target for hackers to gain elevated access into their enterprise's network and if a hacker was able to gain access to these critical datasets they could also could gain access to their entire network.

Also very important was the monitoring of access to Personally Identifiable Information (PII) stored in the DB2 database. Using MEAS, the client is not only able to monitor access to the critical DBV2 databases, but also to individual application programs that access those DB2 databases, sending event information to the SIEM for monitoring, reporting and alerting.

USE CASE #2: This client is a healthcare provider that supports 750K members and payouts over $2.7B in health care benefits. They have been serving their customers for 77 years. MEAS was purchased in December of 2015 because of a compelling event – an audit review. They had a compliance requirement to "monitor security violations". The client's security partner and the SIEM vendor were suggesting that the client "offload all violations to their SIEM" which would check the box from the audit perspective. However, this approach would have been extremely costly and impossible for anyone to actually identify real threats. We were contacted by the partner after they attempted to POC their approach are realized that there was a massive amount of data that would be collected increasing the cost of the SIEM and put their company at risk.

Without a POC, the client purchased MEAS for ACF2. We engaged our collective teams and they were able to quickly architect the solution and identify critical infrastructure that should be monitored that would allow MEAS to monitor violations associated with that infrastructure. The client saved hard dollars on storage associated with supporting their SIEM and also is able to identify relevant violations.

MEAS can support all mainframe security systems such as Top Secret, Top Secret Audit file, ACF2 and RACF allowing companies to filter and monitor security violations. MEAS will allow a company to monitor and alert based on security violations. Companies can monitor specific privilege users for authorized access or unauthorized access.

USE CASE #3: This client contacted us after they published RFIs to support their SIEM requirements that included the mainframe. After a very short POC, MEAS identified files that were being transferred to an organization outside the United States. This was an obvious concern and was escalated to the compliance team for further review. Another requirement was for the company to monitor security violations for each business unit's user access and security controls. MEAS' flexible architecture enabled the company to satisfy this request. MEAS was able to satisfy all of requirements by monitoring their security systems and create output for each SIEM. MEAS also monitors FTP for abnormal FTP activity.

USE CASE #4: Large global bank purchased MEAS to support compliance requirements. Their original use case was to monitor security violations and security events coming from their RACF system. Then they determined they wanted to monitor DB2 data sets that stored critical and compliance data. They were able to deploy the technology quickly and have been adding monitoring capabilities for more mainframe systems.

USE CASE #5: This client is an American multinational insurance corporation with operations in more than 80 countries and jurisdictions and employs 56,400 people. They purchased MEAS to connect CA Compliance manager to their RSA SIEM. During the last two years they are deploying MEAS along with Splunk globally to support their security program. MEAS runs on 38 LPARS that run Top Secret and 10 more running RACF. The original requirement identified to provide security events to their SIEM. They attempted to write code to satisfy their requirement but the quickly realized that the scope of developing and maintaining the code was cost prohibitive and the time to market would be too long. They also need real time capability.