Mainframe Event Acquisition System^{TM} (MEAS^{TM}) technical overview:

MEAS^{TM} is comprised of two major components:

1) MEASMON – This is the programming that executes on each desired LPAR on the customer's mainframe(s). MEASMON is responsible for monitoring SMF, the Master Operator's Console and other input sources.

   At start-up, MEASMON will load the customer's filter definition file, which allows mainframe activities to be specifically targeting for event creation. For example, if a customer desires to create an event for all security related activities, the filter definition file would contain the following parameter.

   ```
   SELEVN=080 ALL SECURITY SMF ACTIVITY
   ```

   When MEASMON identifies a SMF type 80 security record for CA Top Secret or IBM RACF (or type 230 for CA ACF2), MEASMON will create an event from the SMF record and send it to MEASSRVR for further processing.

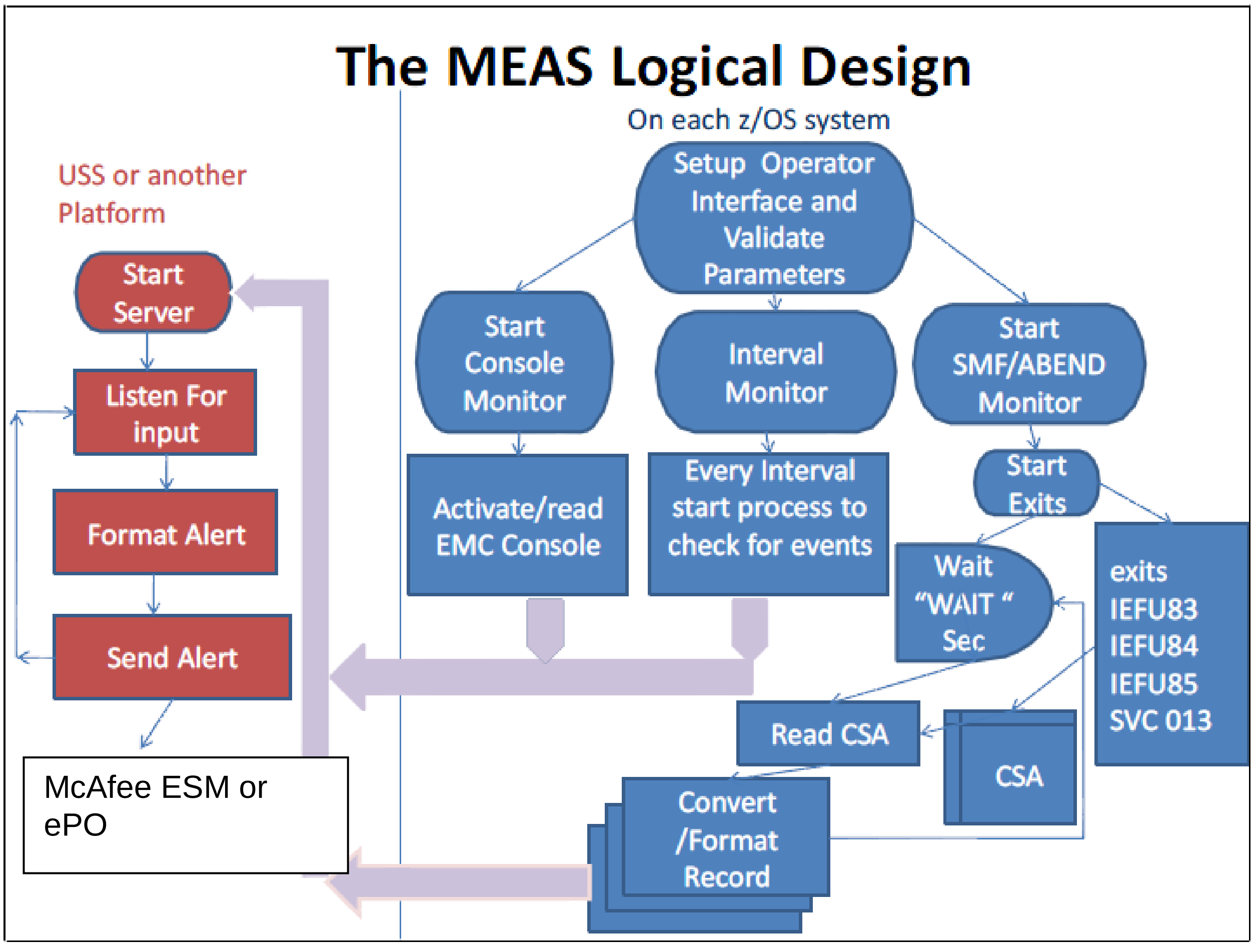
   MEASMON is designed to create events in real-time and is also designed to leverage the customer's System z Integrated Information Processor (zIIP) if available.

   MEASMON also has an interval monitor capability, which allows the function of MEAS^{TM} to be extended to any log file source on z/OS, Unix Systems Services (USS), Linux for System z or other open systems platform.

2) MEASSRVR – MEASSRVR is an open systems component of MEAS^{TM} that performs several distinct functions:
   a. Formats the event record from MEASMON into a standard event record definition known as the Common Event Format (CEF);
   b. The severity level for an event is set;
   c. The event is transmitted to McAfee ESM or McAfee ePO.

   Depending upon the number of mainframe LPAR's being monitored, it may be necessary to have multiple MEASSRVR instances to manage the workload from multiple MEASMON instances.

   MEASSRVR is written in Java, so if executed on a Linux for System z instance, it is eligible to execute in a System z Application Assist Processor (zAAP) if available.



In this flowchart, the **blue** symbols represent processes that run on each z/OS system (LPAR) being monitored, the **purple** arrows represent the TCP/IP network, and the **red** symbols represent the processes that run on the server that places the events in a format and location where the events are picked up by the "Security Information and Event Management" technology. The following briefly describe the processes:

1. Monitors detect selected activity and send it to a specified port and address in the TCP/IP network.

2. One or more servers receive this data, format this activity in CEF format, and place it where the McAfee ESM or McAfee ePO has been setup to look for this information.

Product names are registered trademarks of their respective companies

MEAS™

703-825-1202
813-258-0488
sales@meas-info.com