ACTION SOFTWARE INTERNATIONAL

Real-Time
System Management Solutions
for z/OS Systems

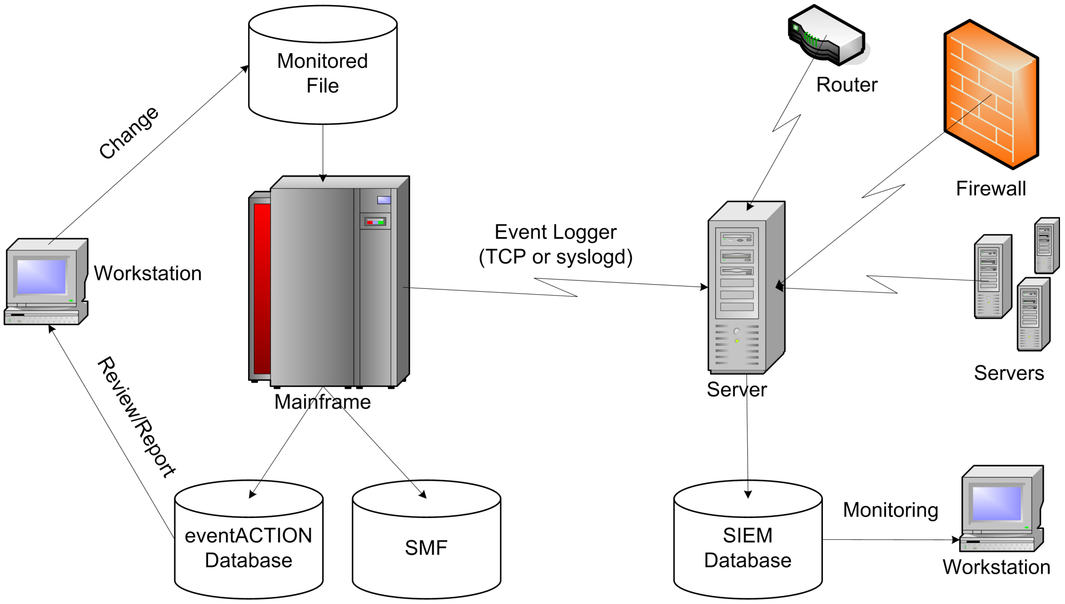
SOLUTION PREVIEW – EVENT LOGGER

Challenge

Large IT infrastructures are under constant threat of intrusions. Many organizations are turning to SIEM or similar products to aggregate and analyze events from across the enterprise, in order to detect and handle threats in a timely manner. Mainframes typically contain an organization's most valuable and sensitive data, and it is vital that both successful and unsuccessful accesses to key mainframe resources be included in any aggregate view of the threat landscape. There are significant challenges in getting mainframe event data to these products due to the unique attributes of mainframe data such as EBCDIC character encoding and unique number representation formats, as well as security environments that are unlike those of other platforms.

Solution

eventACTION for z/OS MVS and **ussACTION** for z/OS UNIX (USS) allow a site to define what resources are important, and focus on events affecting those resources. Changes to these resources are tracked and controlled in real time according to the site's specifications.



The new Event Logger component of **eventACTION** and **ussACTION** will allow information about tracked events, both successful and unsuccessful, to be propagated to a variety of destinations, initially including:

- SMF;
- UNIX syslog; and
- Remote systems via TCP.

Network destinations use TCP/IP services provided by IBM z/OS Communications Server.

The TCP and syslog destinations permit sending event information directly to off-platform systems, such as a SIEM product. The SMF destination supports all current SMF facilities, including the high-performance SMF real-time interface. Additional destinations will be added in subsequent Event Logger enhancements.

eventACTION and **ussACTION** tracking and control facilities provide the ability to quickly analyze and manage changes to key resources on z/OS systems, with minimal effort required to define what resources are important. Event Logger allows that same event information to be propagated to enterprise-wide repositories immediately as the events occur, thus enabling changes to key z/OS resources to be a part of real time threat analysis for the enterprise as a whole, without these events being buried in a huge volume of unimportant events.

The initial types of events that can be propagated include:

- Changes to MVS data sets and members;
- Rejected changes to MVS data sets and members;
- Changes to USS directories and files; and
- Rejected changes to USS directories and files.

In the above, “changes” includes create, rename, update and delete activities. For USS, it also includes attribute changes, chmod, chown, mount, umount, etc.

Any mainframe-related events highlighted by the SIEM or similar product can be further investigated using **eventACTION** and **ussACTION**. Changes can be displayed using flexible search criteria, and can be analyzed in detail using compare with generations of backups automatically taken by **eventACTION** and **ussACTION** as changes occur. Incorrect changes can also be backed out using these backups.

Example

An installation specifies to eventACTION that all data sets in the system parmlib concatenation should be tracked, and that tracked changes should be sent to a SIEM product via TCP.

A user changes several members of parmlib library SYS1.PARMLIB. eventACTION detects the member changes.

eventACTION saves information in its database about the changes, including who made them, and when and how they were made, and captures backups of the changes.

eventACTION’s Event Logger component transforms the event data to a format usable by the SIEM product and transmits the data to the SIEM.

The SIEM product incorporates the eventACTION information in its event analysis to help detect threats.

Determination of validity of z/OS systems changes requires z/OS subject matter experts. The event information and the backups in eventACTION allow the details of the changes to be analyzed. Erroneous changes can be backed out using the backups, and malicious changes can be recognized immediately.

Conclusion

Mainframes generally contain an enterprise’s most important data. When a non-mainframe product is being used to perform security monitoring, it is vital that mainframe events are included in the monitoring. The Event Logger feature reduces the effort required to include changes to important z/OS resources in enterprise-wide security monitoring.

Action Software International
Tel: (800) 821-4551
Fax: (905) 470-6507
actionsoftware.com