SDS VITALSIGNS SIEM AGENT™ for z/OS
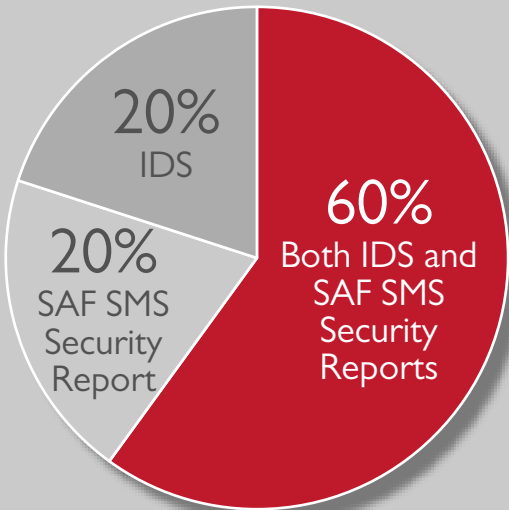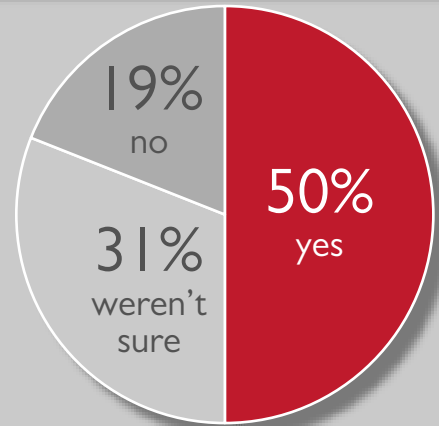
SIEM Results from 2018 Enterprise Systems Media Survey

19% Organizations with a z/OS SIEM solution in place
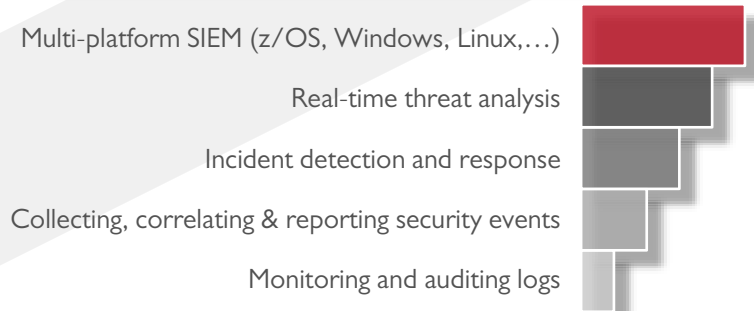
- 16% were actively looking at filling z/OS SIEM need
- 31% didn't have z/OS SIEM solution
- 34% weren't sure

Organizations with an enterprise SIEM in place

- 19% no
- 31% weren't sure
- 50% yes

Current methods used to monitor z/OS security events

- 20% IDS
- 20% SAF SMS Security Report
- 60% Both IDS and SAF SMS Security Reports

SIEM Solution Requirements
(ranked from most to least important)

- Multi-platform SIEM (z/OS, Windows, Linux,…)
- Real-time threat analysis
- Incident detection and response
- Collecting, correlating & reporting security events
- Monitoring and auditing logs

Mainframe SIEM Areas of Interest

Batch	SAF (ie. RACF)	WTO/ console messages	Data Set Access	USS	CICS	Task-related events (ie. TSP)	MQSeries	Db2