Moving from SIEM to Security Analytics: Evolution or Starting Over?

John Pescatore, Director, SANS

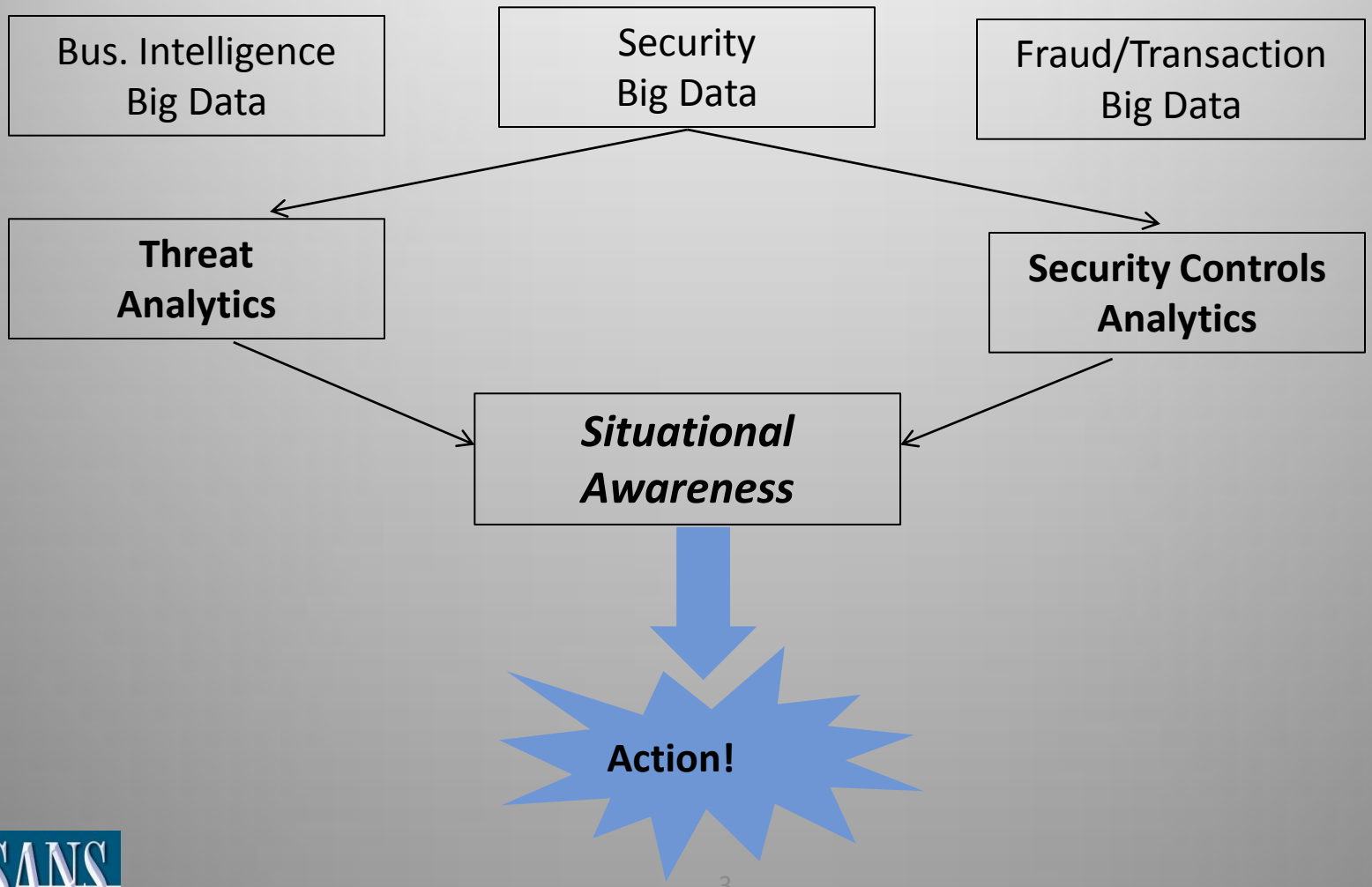
SANS

Our Panel

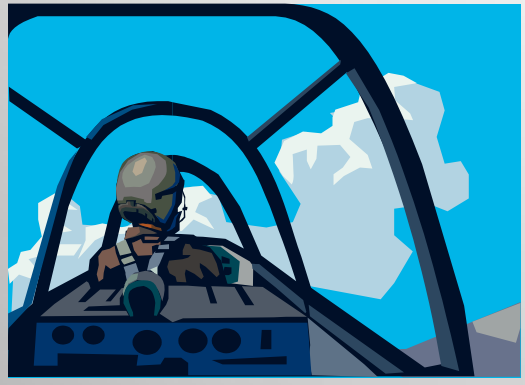
- Salo Fajer, Intel Security
- Ron Gula, Tenable
- Adam Meyers, Crowdstrike

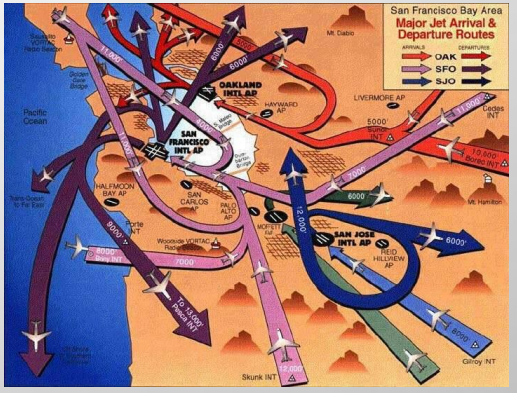
SANS

From Data to Action



Defining Situational Awareness

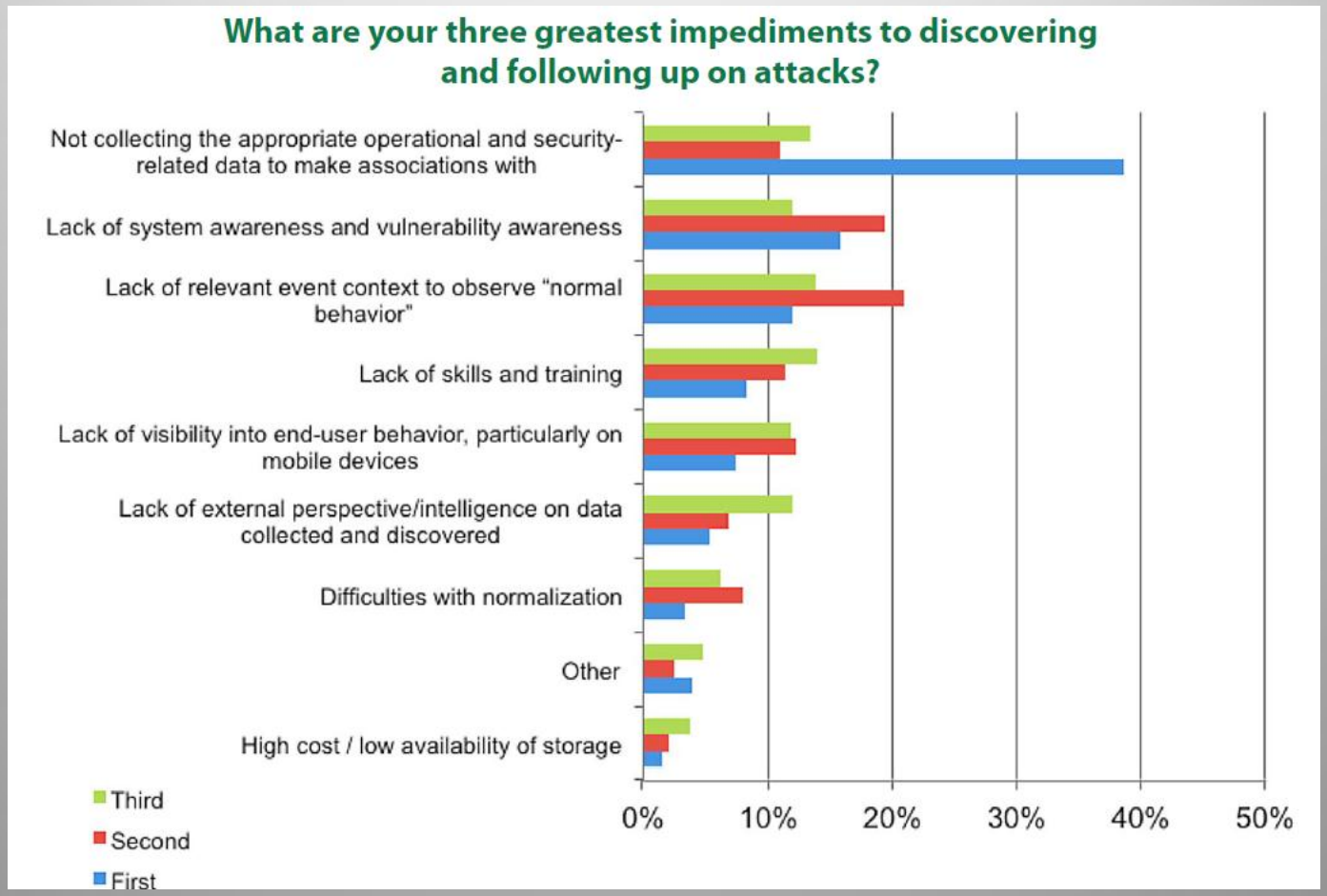




- **Pre-flight**: plan safest route
- **In flight**: Decreasing reaction time so that mission gets accomplished, pilot returns safely
- **Post-flight**: do better next time

SANS

Impediments to Action



Data Sources

What types of operational and security reporting data are you collecting for use in security analytics today, and what do you anticipate you'll be collecting 12 months from now?

Answer Options	Currently collect	Plan to collect within 12 months	Don't plan to collect	Unknown
Log data from network (routers/switches) and servers, applications and/or endpoints	77%	15%	2%	4%
Monitoring data provided through firewalls, network-based vulnerability scanners, IDS/ IPS, UTMs, etc.	77%	16%	1%	4%
Access data from applications and access control systems	45%	27%	12%	12%
Unstructured data-at-rest and RAM data from endpoints (servers and end-user devices)	12%	19%	39%	24%
Security assessment data from endpoint (aka from NAC/MDM scans), application and server monitoring tools	37%	29%	15%	16%
Assessment and exception data (not on the whitelist of approved behaviors) taken from mobile/BYOD endpoints (aka from NAC/ MDM scans)	14%	25%	30%	24%
Monitoring and exception data pertaining to internal virtual and cloud environments	22%	27%	22%	24%
Monitoring and exception data pertaining to public cloud usage	14%	17%	37%	28%
Other	3%	2%	4%	12%

SANS

Tools and Satisfaction