JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Data Analytics

Security Architecture & Tool Sets

Data Analytics

- Integrating logs across the devices provides the most value and information
- Manual review of logs is time consuming
- Automated systems can help prioritize items for review based on heuristics and previous signatures created
- You need to conduct data aggregation and correlation, trend analysis, and historical analysis

Data Aggregation and Correlation

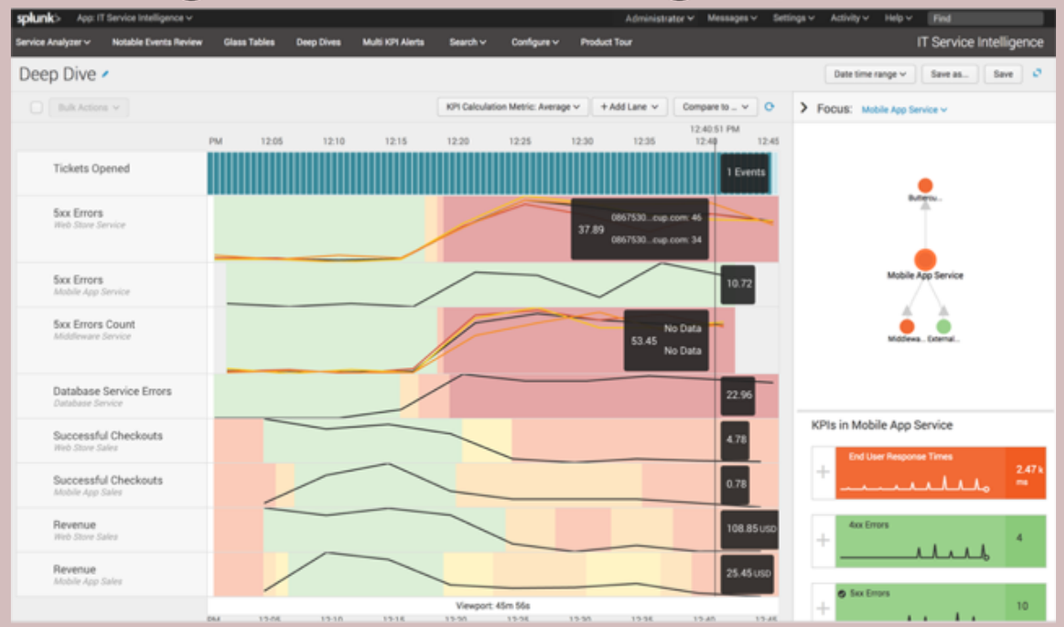
- Combine data from multiple sources to identify events impacting different systems
  - System logs, authentication logs, application logs, event logs, and others into central analysis node

- Effective as a detective control

Trend Analysis

- Analyzes system, events, and devices to detect trends and patterns

- Identifies issues that are outside of expected growth or usage patterns



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Historical Analysis

- Analyzes system, events, and devices over time to detect trends and patterns

- Helpful during incident responses as it looks back over a longer period of time

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE