2015 CTI Survey Results Preview

Michael Cloppert

report author: Dave Shackleford
Objectives

- General; CTI as a domain:
  - Increase clarity
  - Reflect overall maturity

- Specific; survey measurables:
  - Determine state of CTI policies, practices
  - Measure perceived value of CTI
Cohort: 326 qualified respondents

**Primary Industry**
- Govt
- IT
- EDU
- Mfg
- Health
- Telecom
- Consult

**Operating Regions**
- US
- Europe
- APAC
- CA
- S/C Amer
- Mid East
- AU/NZ
- Africa
- Other
Organizational Investment in CTI

- **64%** have some investment in CTI
- **25%** seeking to invest in CTI
- **7%** have no plans
Can you estimate how CTI tools and processes have improved your organization’s response to events in terms of context, accuracy, and/or speed?

- Plurality unsure of benefit
- Immature metrics in CTI
- Question framing
- Majority estimate some benefit
Sources for Threat Intel

- Fewer collect internal intelligence
  - Higher value
  - Requires maturity
- Many orgs multi-sourced
  - Data management challenges
Enabling Platforms for CTI

- Multiple platforms seem common
- Applicable to many CND/IR aspects
- 25% home-grown: capability gap?
Detailed report released soon!

- Part I: Definitions, Tools, Standards
  - Tuesday, Feb. 17, 1 PM EDT with Dave Shackleford

- Part II: Best Practices to Improve Incident Detection and Response
  - Thursday, Feb. 19 at 1 PM EDT with Dave Shackleford