TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

CYBER THREAT INTELLIGENCE SHARING AT WIRE SPEED

NOVEMBER, 13, 2014

SHIMON MODI, PH.D.

SECURITY R&D MANAGER, ACCENTURE TECHNOLOGY LABS

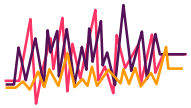
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

THREAT INTELLIGENCE ENABLE ORGANIZATIONS TO

Understand cyber activity that is being observed

Prioritize threats and vulnerabilities that need to monitored

Tactical



Gain a historical perspective of threat activity

Comprehend how attacker moves along cyber kill chain

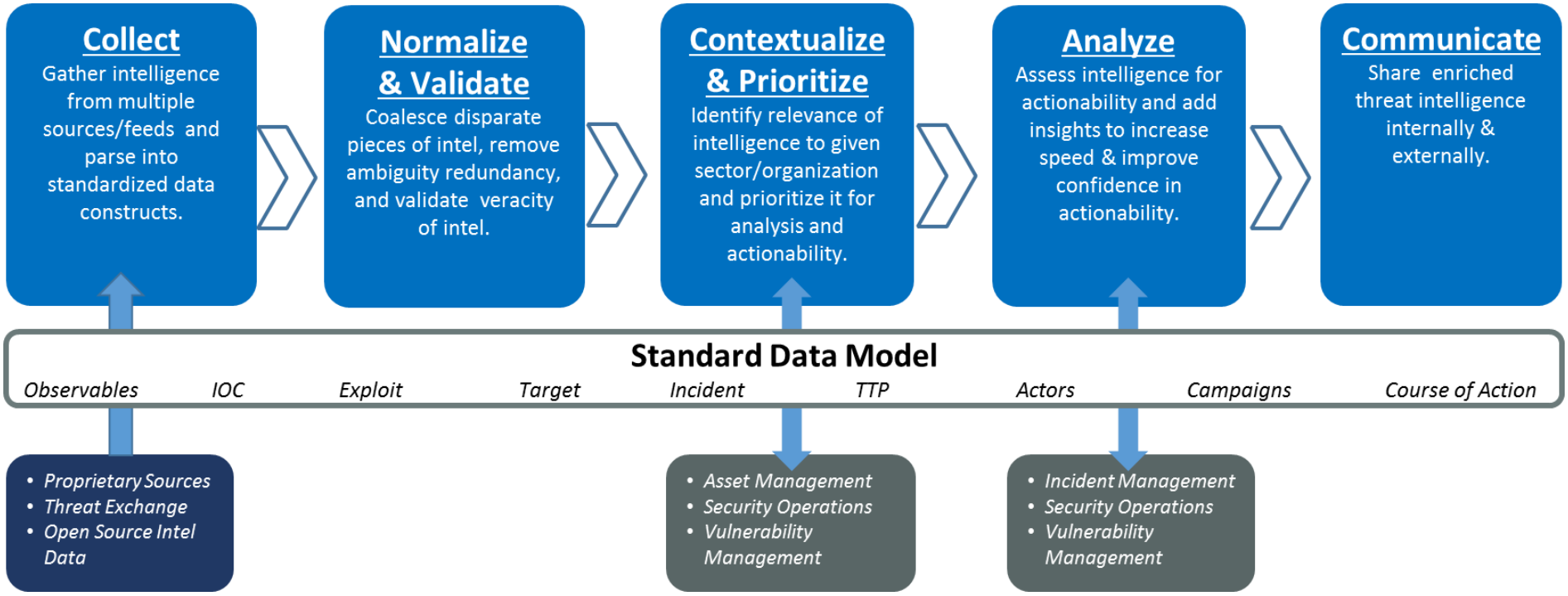
Operational

Understand motives of the threat actor

Determine mitigation action, either proactive or reactive, against threat activity

Strategic

OPERATIONALIZE THREAT INTELLIGENCE



ENHANCING CYBER THREAT SHARING

- Collecting & Sharing threat intelligence with trusted partners
  - Standards based M2M sharing
    - CyBOX, STIX, TAXII, CRISP
  - Connecting electricity sector organizations using standardized representations
    - ES-ISAC, MS-ISAC, ICS-CERT
- Speeding exchange of threat intelligence
  - Automate process of filtering, analysis and distribution