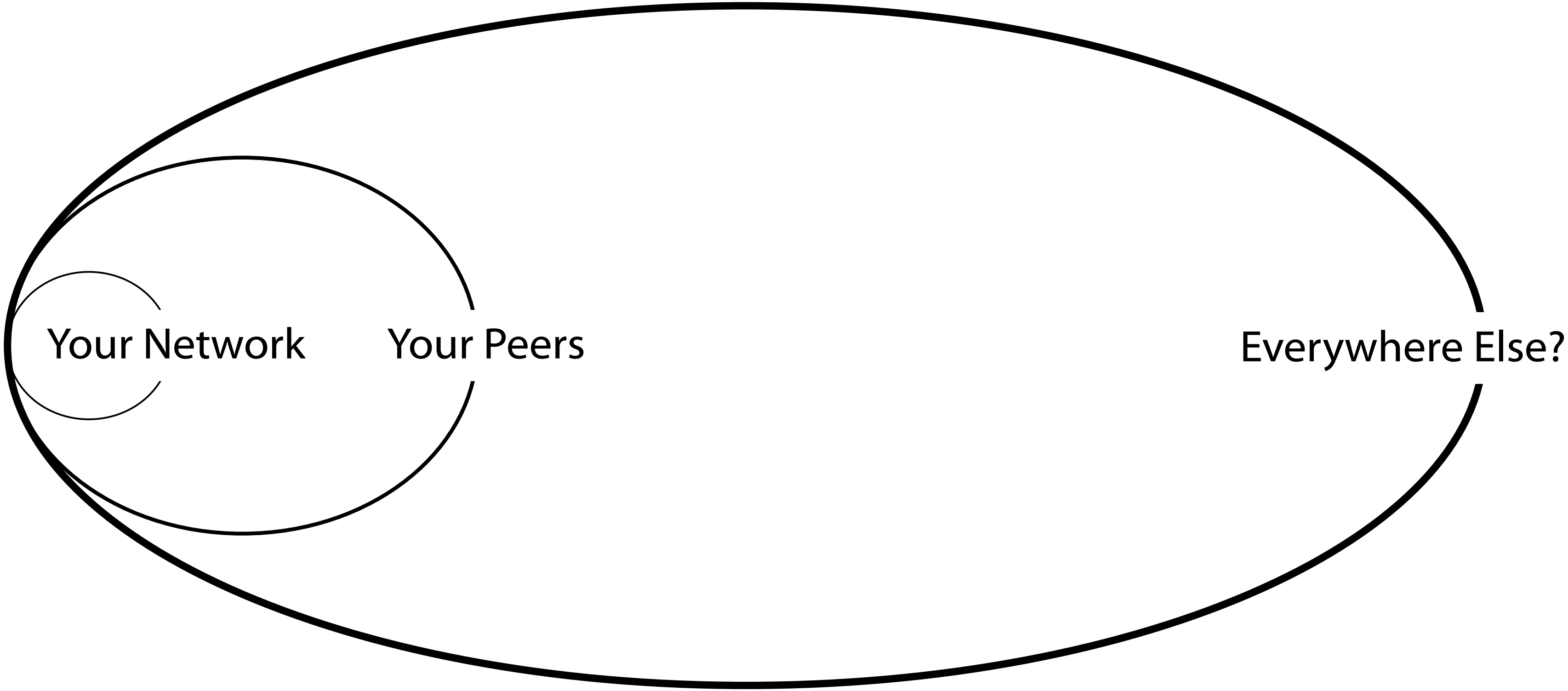
Anticipating Novel Cyber Espionage Threats

John Hultquist, iSIGHT Partners

Sources of Intelligence Insight



Iranian Aggression

- Stuxnet
- Saudi Aramco and Rasgas Attack
- Operation Ababil
- Sands Casino
- Probing of Critical Infrastructure

Sandworm Team and Critical Infrastructure

- Targeting of US SCADA
- Targeting of Ukraine Energy and media
- Destructive event against Ukraine media
- Destructive event against Ukraine energy
- Definite implications for the US
  - Energy
  - Media

SANDWORM TEAM

Driving Factors and Attracting Factors

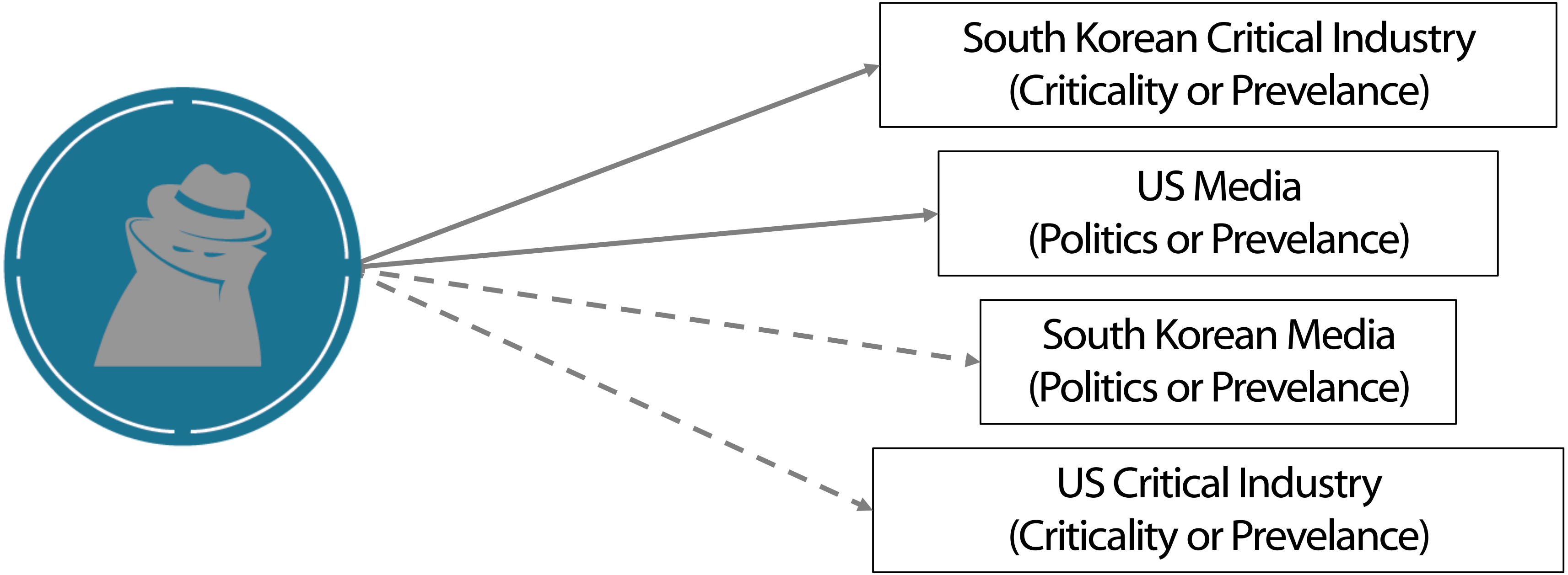
Driving Threat Actors

- Regional
  - Origins
  - Nascent
  - Regional Focus
- Specialization
  - PII
  - Economics
  - IP
  - SCADA
  - Aggressive, hacktivist-like activity

Attracting Threat Actors

- Sensitive policy and military information
- Presence
- Politics
- Platform and Access
- Prevelance and Criticality
- Research and Development

Scenario One



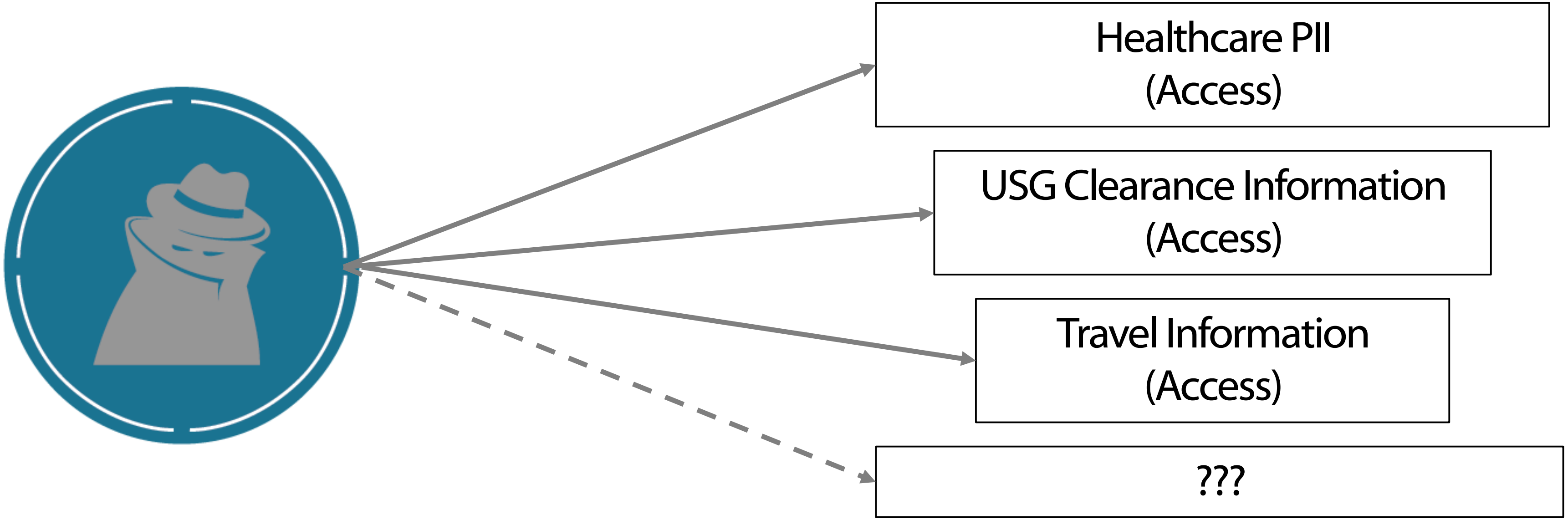
South Korean Critical Industry
(Criticality or Prevelance)

US Media
(Politics or Prevelance)

South Korean Media
(Politics or Prevelance)

US Critical Industry
(Criticality or Prevelance)

Scenario Two



Healthcare PII
(Access)

USG Clearance Information
(Access)

Travel Information
(Access)

???

So what now?

- Assess thyself
- Assess threats by why rather than who
- Identify canaries
- Identify significant threat sources
- Focus on those sources
  - What tools do they use?
  - What TTPs do they use?
  - What IOCs can you gather?

Thank you!

jhultquist@isightpartners.com