Back to Sun Tzu

Knowing the Enemy & Knowing Yourself

Col(ret) Joe Wingo
Director of Strategy, Armis Federal LLC

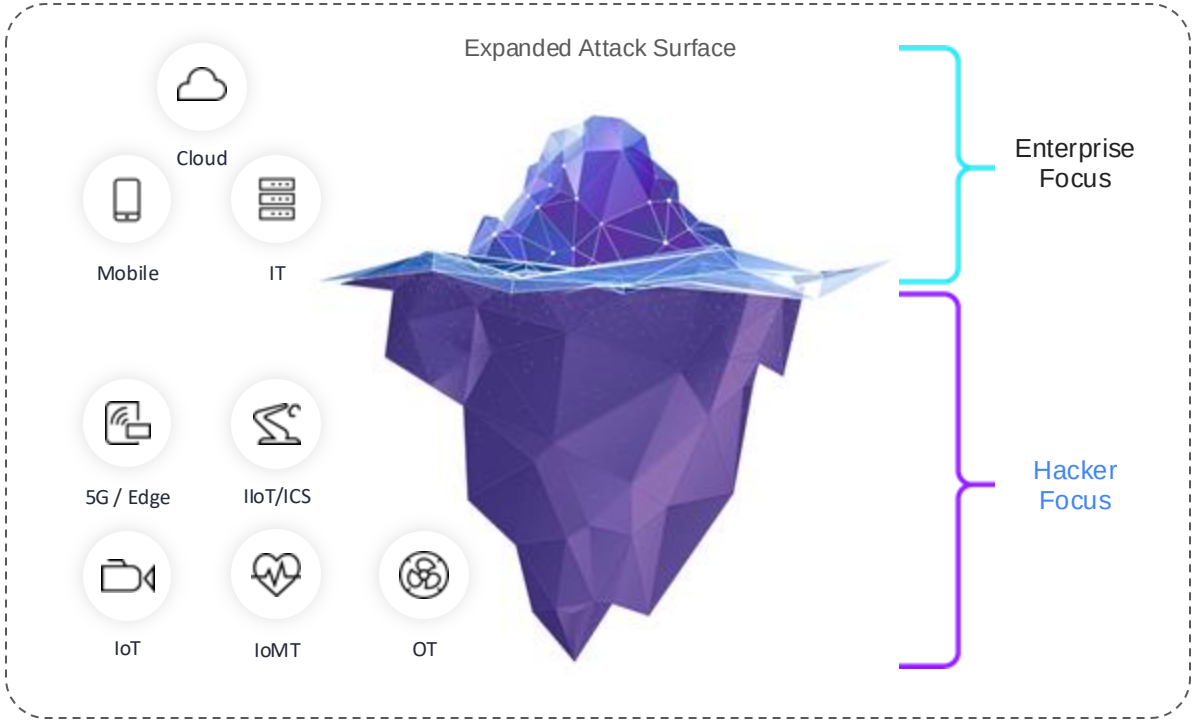
"If you know your enemy and know yourself, you need not fear the result of 100 battles." - Sun Tzu

- Knowing Ourselves - Deep Asset Intelligence
  - Complete situational awareness of every IT, OT, IoT and IoMT asset in your cyber terrain
  - Complete situational awareness of the traffic across your network

- Knowing the Adversary - Threat/Vulnerability Intelligence
  - Insights into an adversary's targeting and TTP development
  - Understand intent and vector before they attack

Cyber Attack Surface

More Blind Spots, More Complexity, More Attacks



3x more non-IT/Mobile assets by 2025

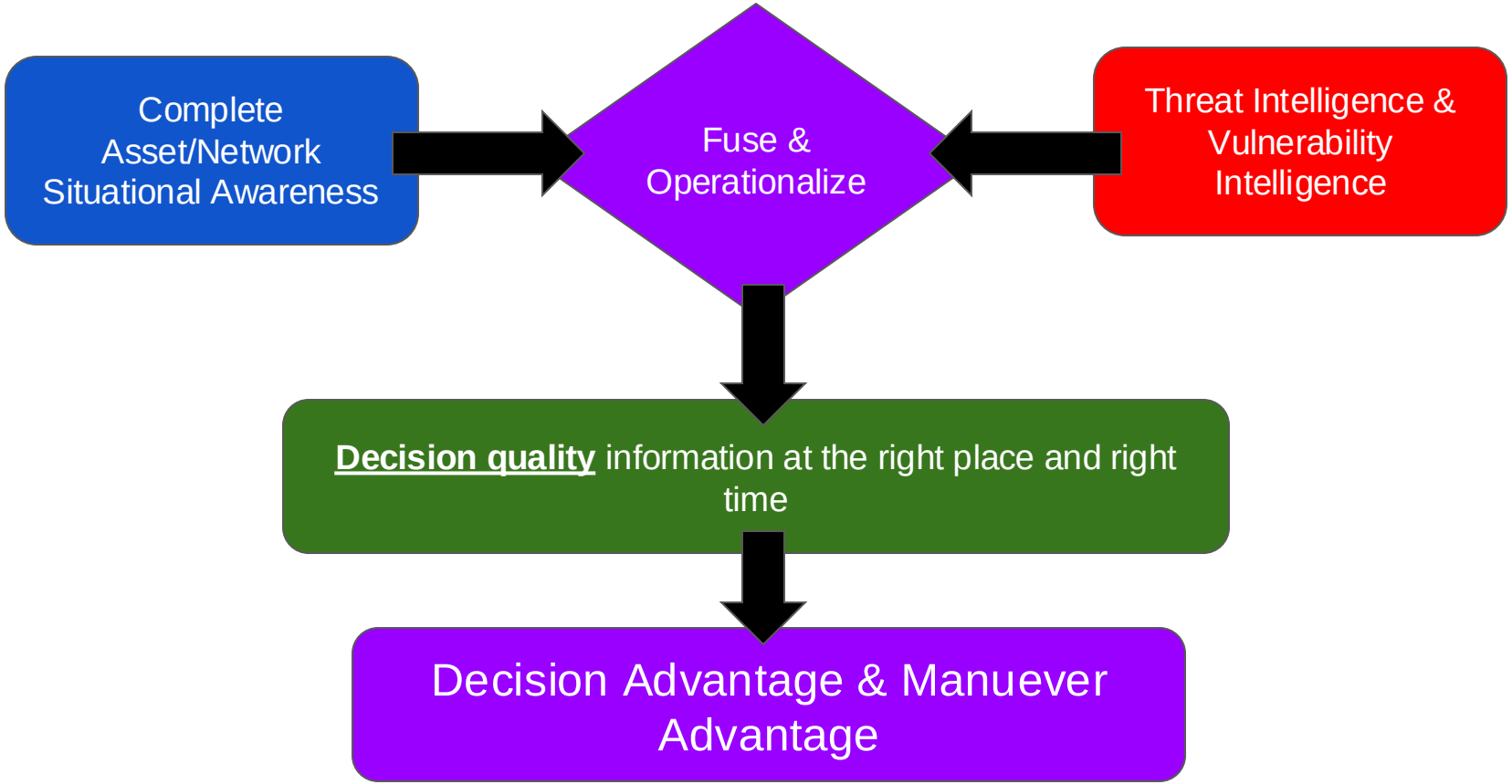
2x the volume of cyber attacks

80% of assets are unseen or unmanaged

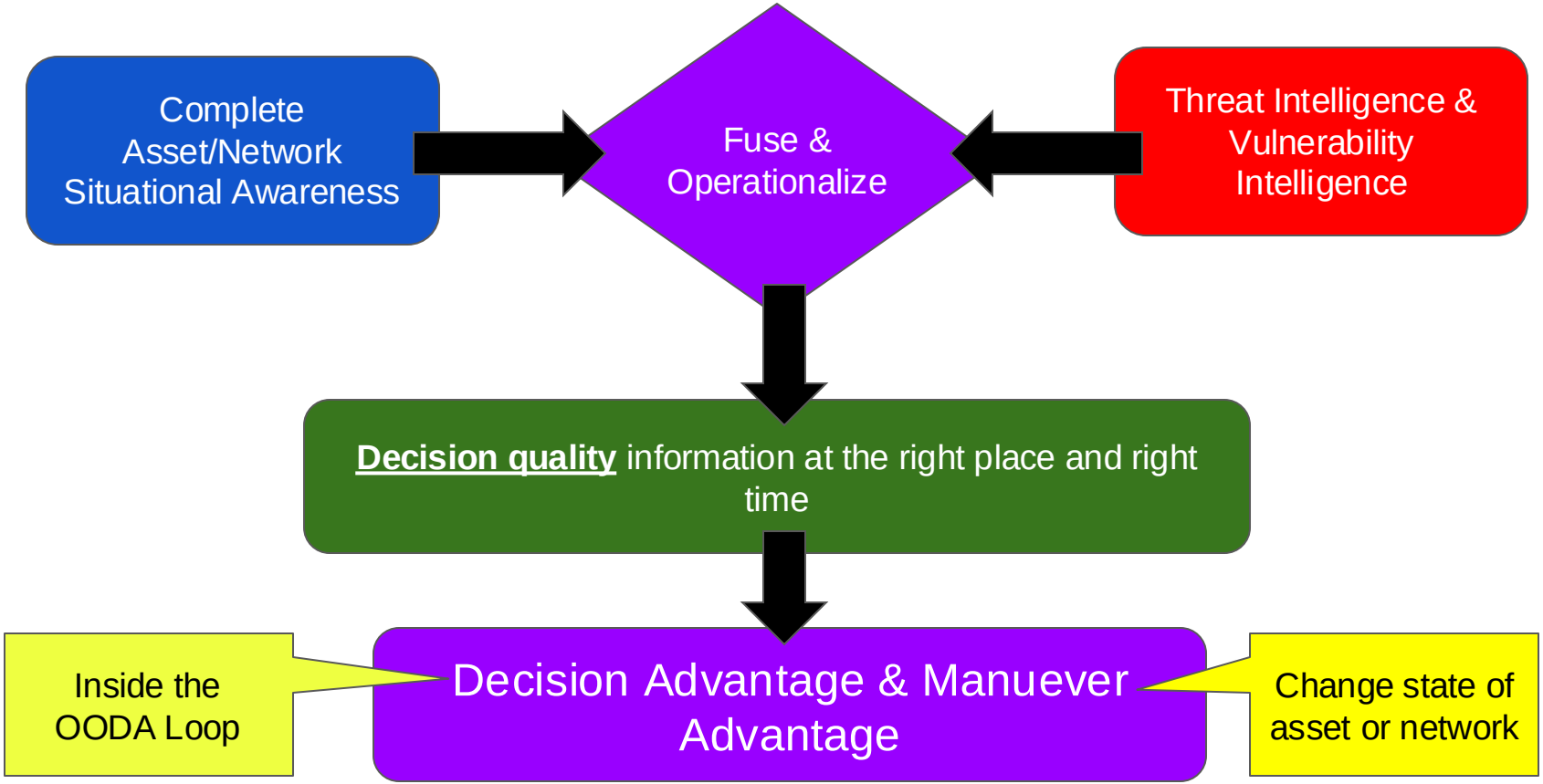
“Good” Vulnerability Intelligence

- Must come BEFORE the attack
  - Duck and Cover alarms that happen after the rockets land are no good
- Must be relevant to my cyber terrain
  - What are the specific types of assets being targeted?
- Must provide the TTP in use
  - Zero day?
  - Existing CVE weaponization?
  - New weaponization of old CVE?
- Must be provided to the right opertator
  - Formatted for easy ingestion
  - Tyranny of Tear Lines

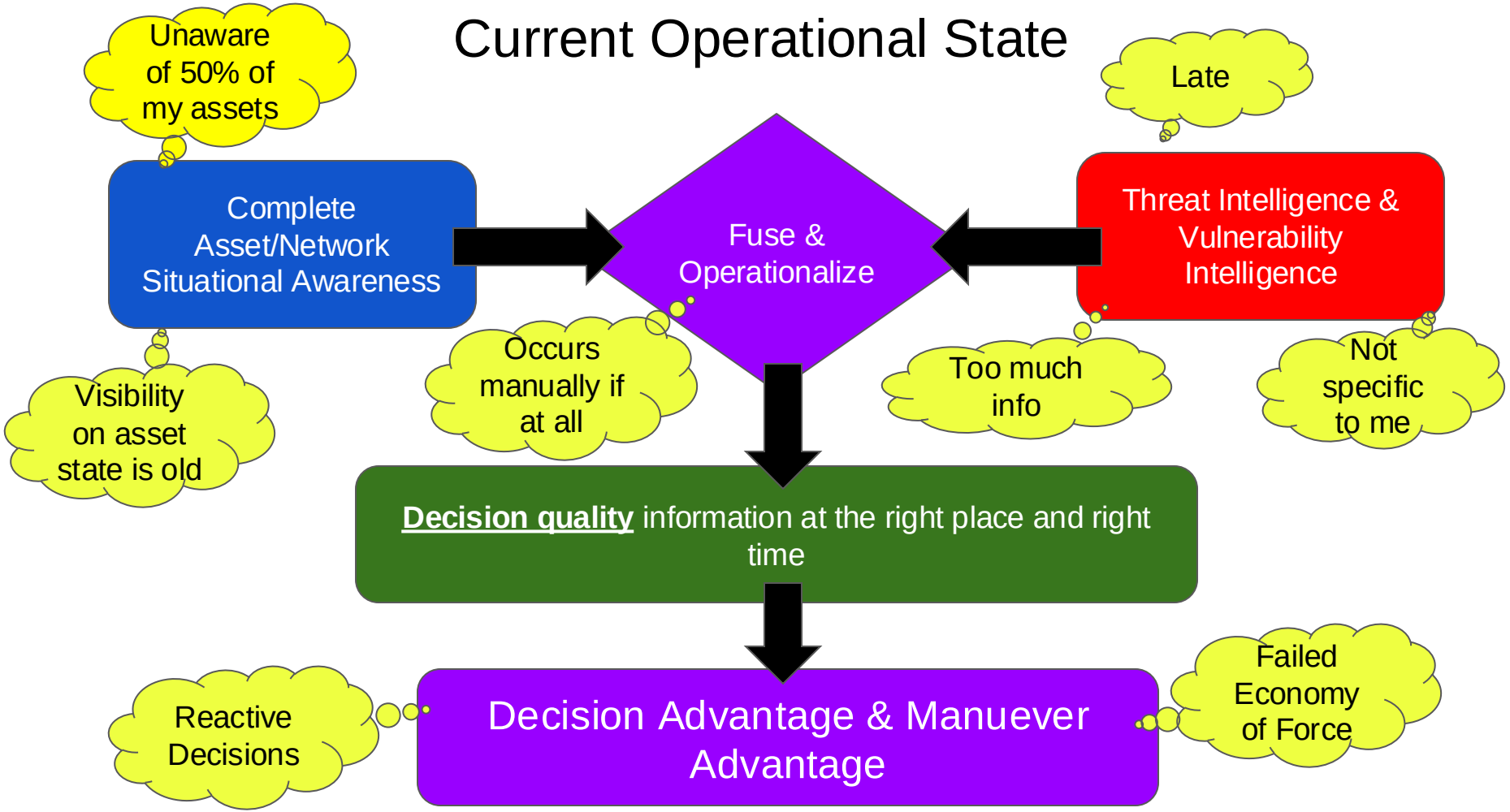
Desired Operational State



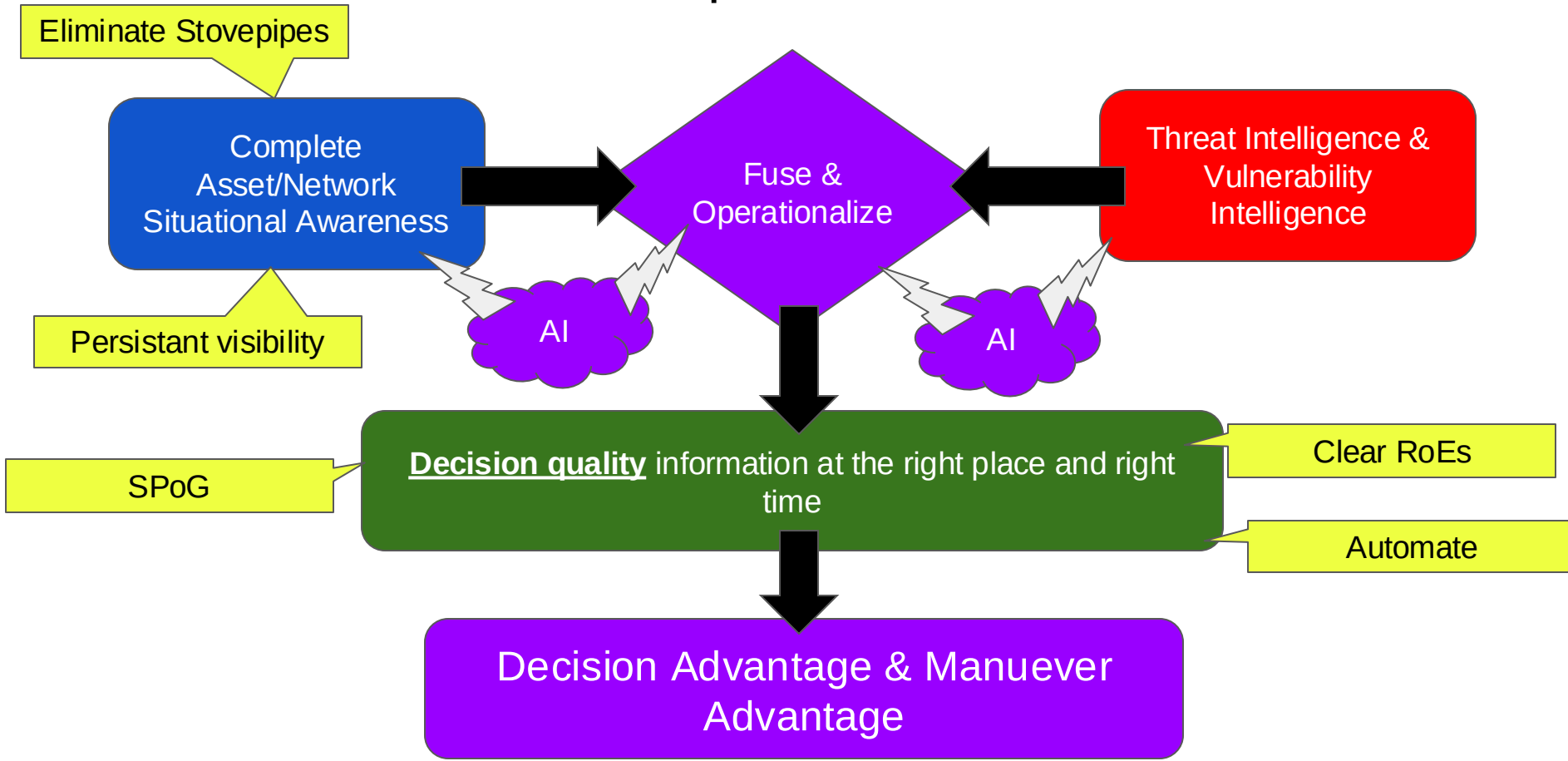
Desired Operational State



Current Operational State



Desired Operational State



Questions?