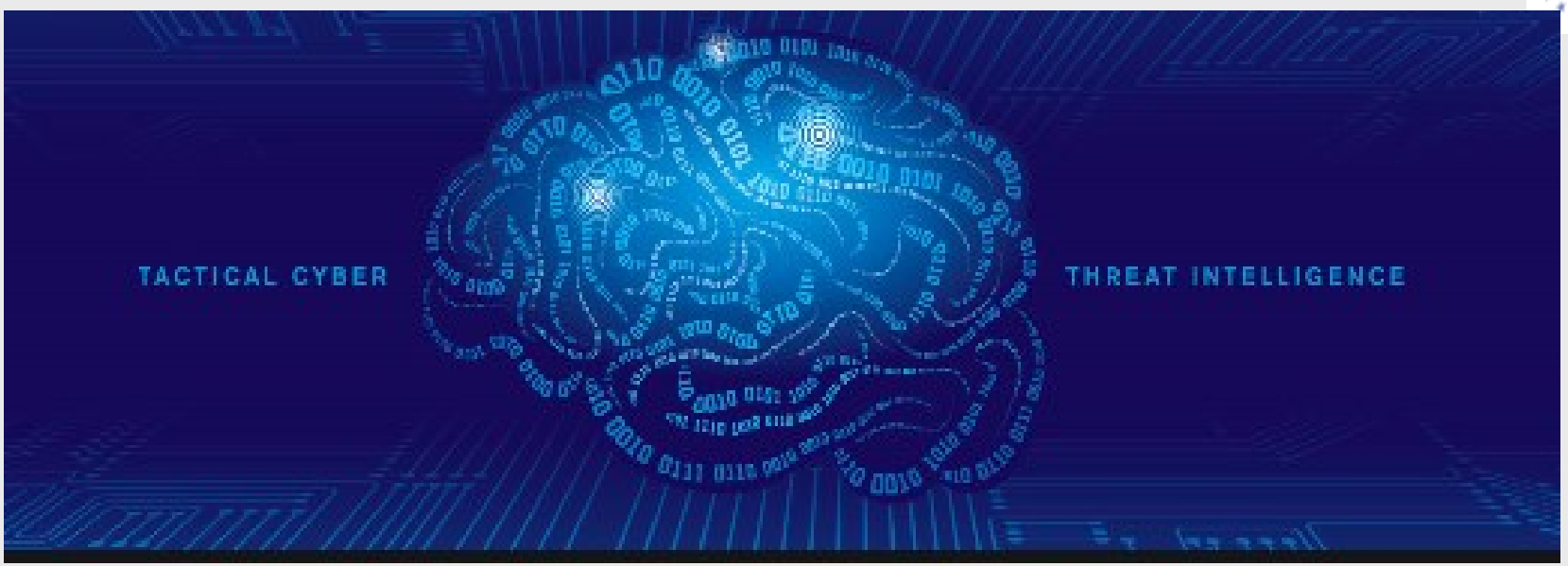
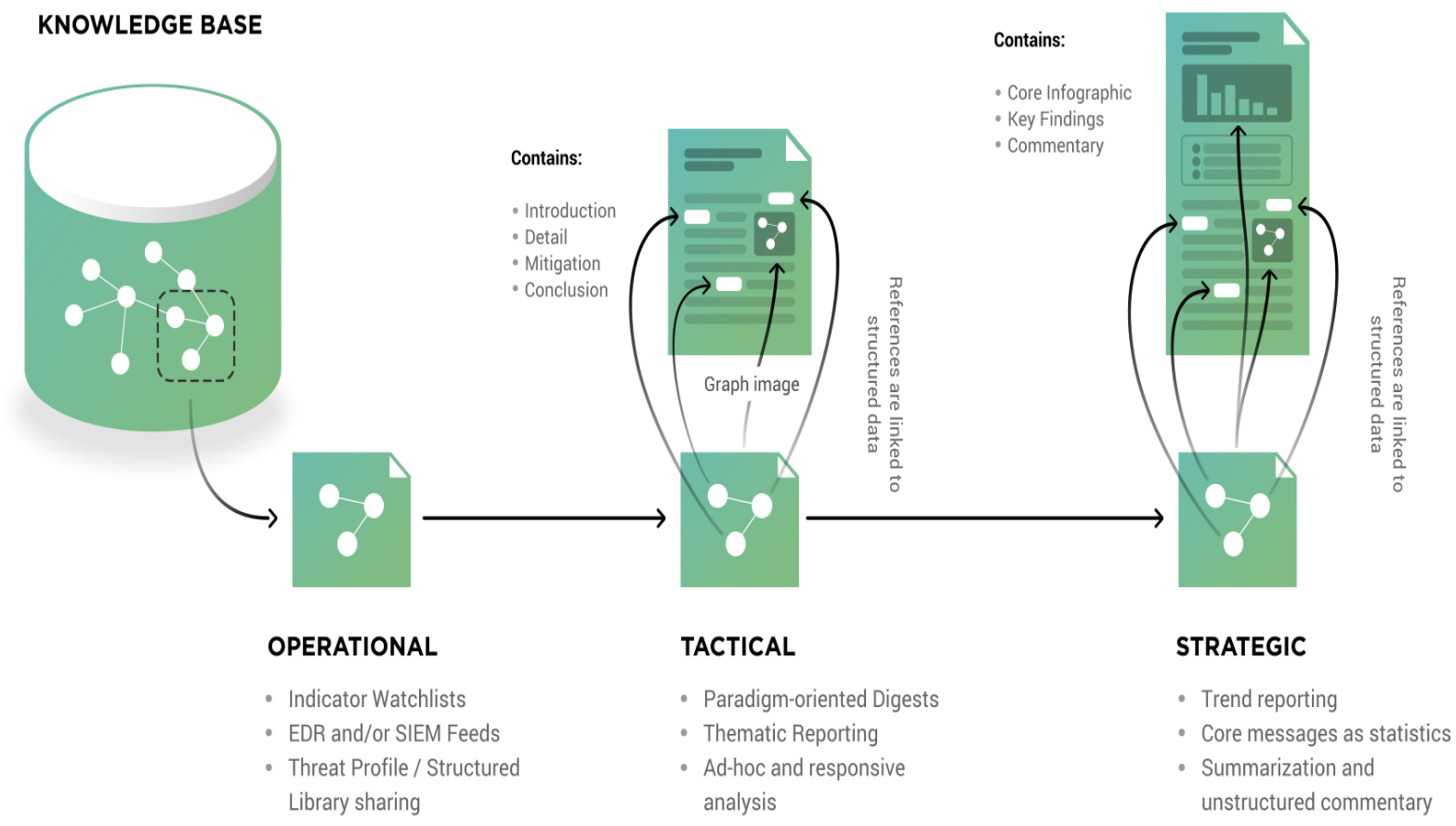



# Embedding CTI in security organisation

***Use CTI to improve your (security) processes***

Paul Samwel, Chris O'Brian, Tiernan Connolly, Richard Kerkdijk

# Chris (Eclectic IQ): structured products.



# Solution:
# Use the Cybercrime Kill Chain

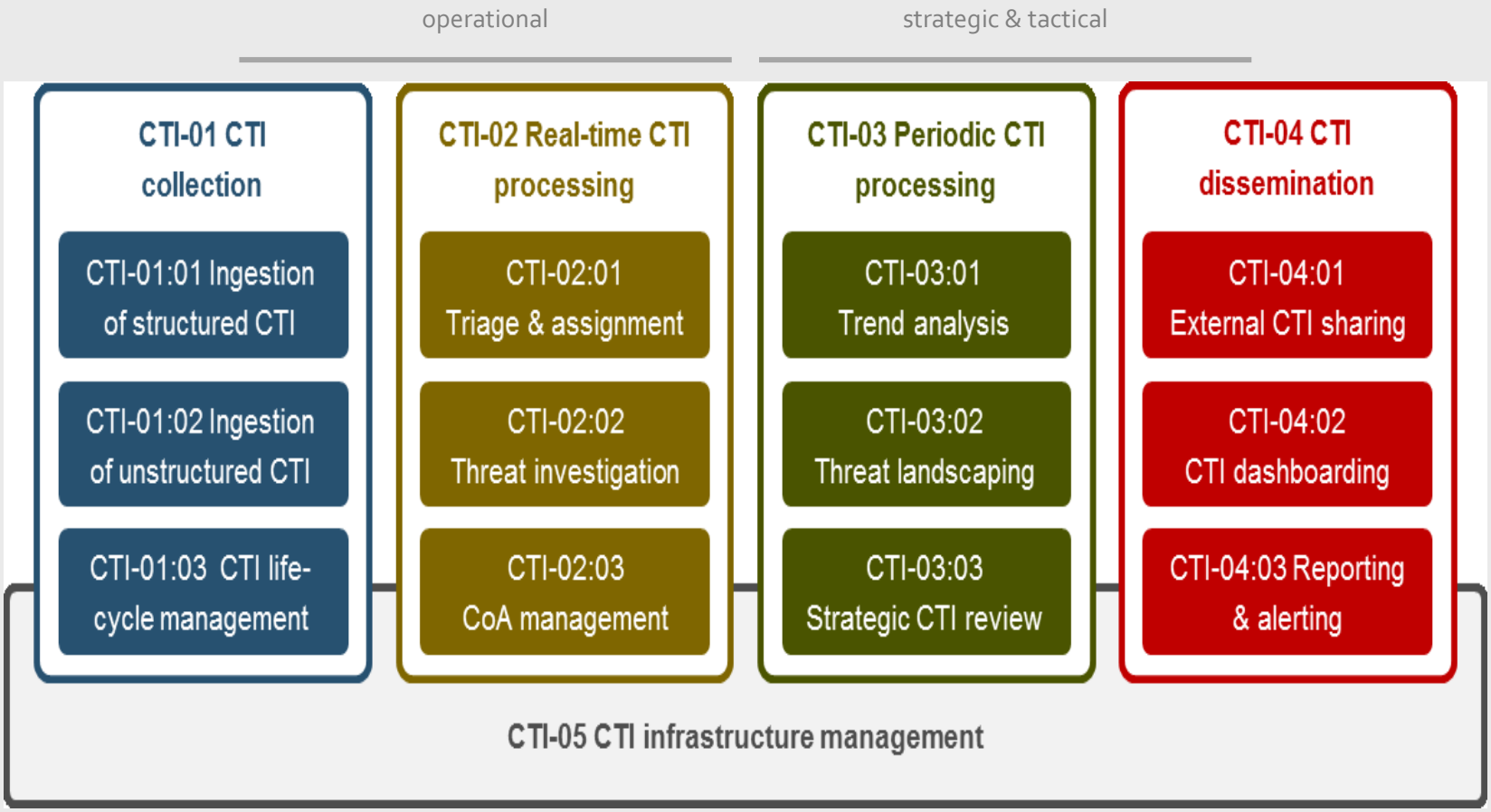
Cyber Threat Intelligence


1. Find crown Jewels
2. Find relevant MO
3. Find Common TTP
4. Find Controls to break TTP
5. Implement controls
6. **Reduce Risk**

Priorities

# Translating Intel for Business


# CTI capability framework



# Summary

**Current focus:**

- Feeding people/systems with Intel = Sharing
- Some operational improvements (feeding detection)

**Missing:**

- Focus on Actions
- Visible results at Tactical & Strategic level
- Business Focus = Risk Reduction
- Acknowledged model for CTI operations.

**From Actionable to Action:**

- From **structured input** (STIX) to **structured output**
- CTI **Key Performance indicators** that measure **Risk Reduction**
- Make **Action** items in CTI framework more **Visible**
- Introduce CTI framework **in Enisa products**