R-CISC

WE NEED TO TALK …

WENDY NATHER

RESEARCH DIRECTOR

FROM GOSSIP TO GROWNUP

(Monday morning at the SOC)

FLIPPING THE INFORMATION ASYMMETRY

They only have
to be right once

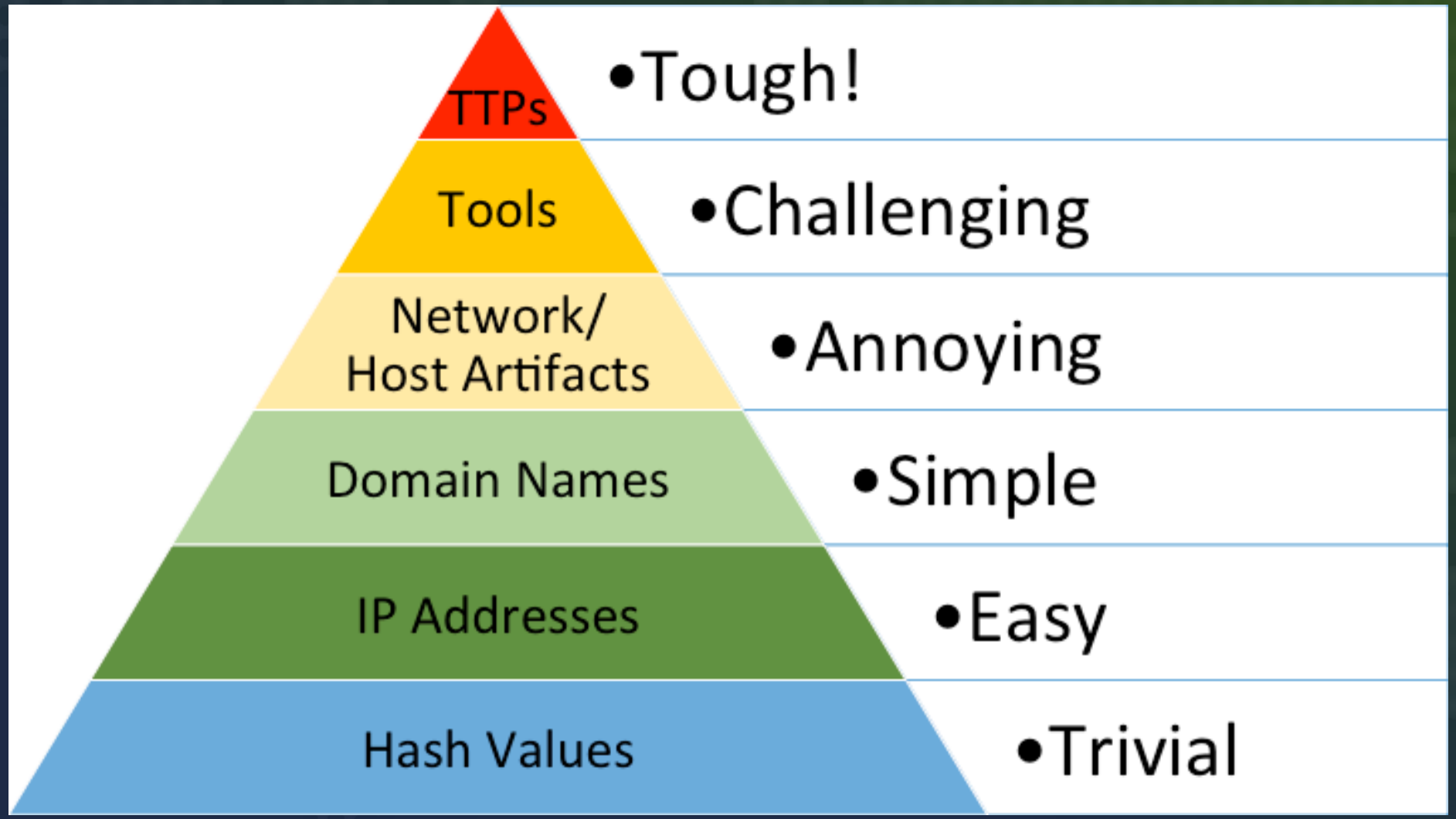
They only have
to mess up once

FLIPPING THE INFORMATION ASYMMETRY

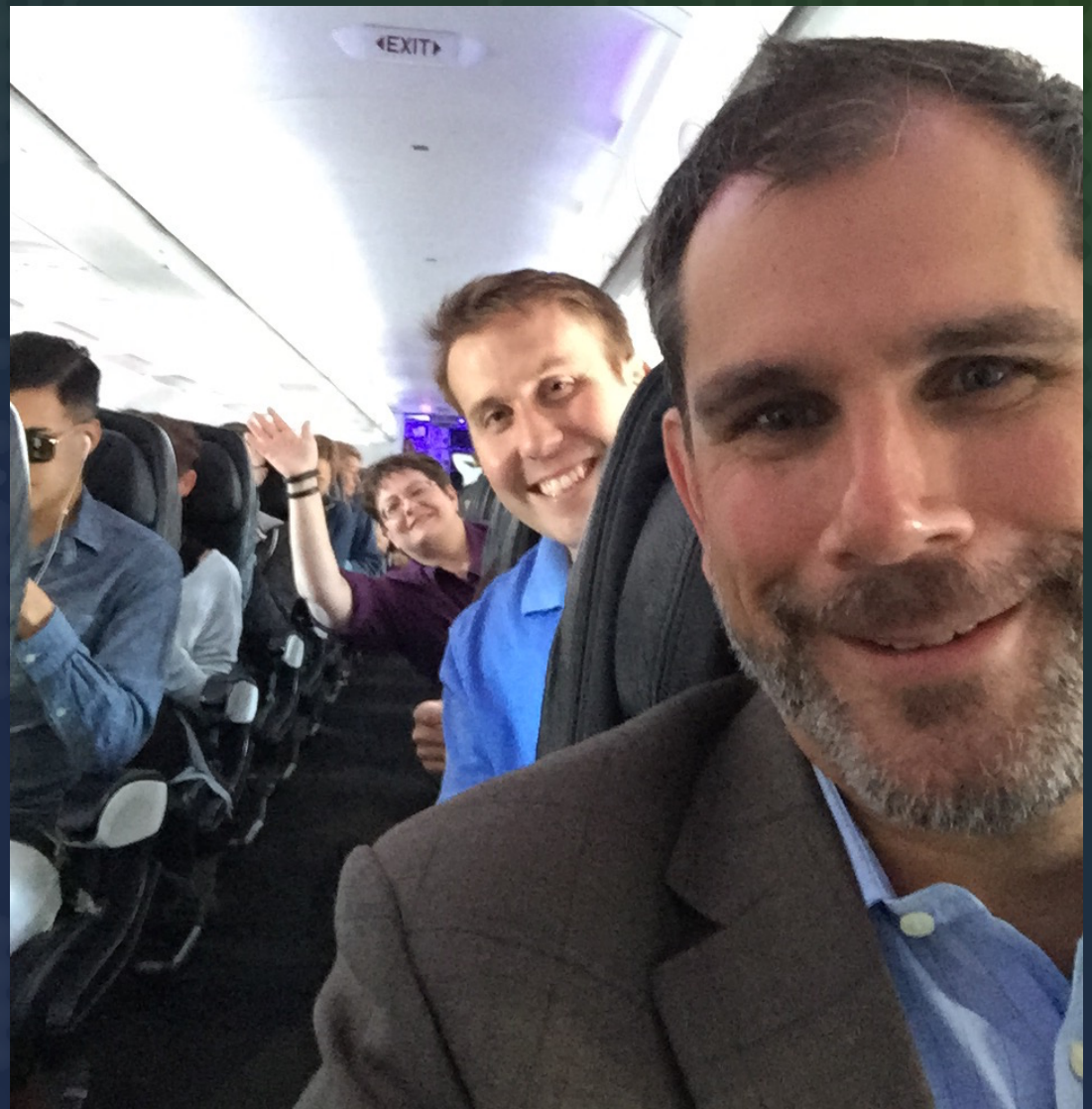
They only have to mess up once

They only have to be right once

DAVID J. BIANCO'S PYRAMID OF PAIN



R-CISC ON A PLANE



BRINGING UP ISAC

- Spun off from Retail Industry Leaders Association (RILA) in 2014
- Seed funding from top retailers
- Operational in early 2015
- Currently at ~80 members
- Board members include Target, Walgreens, JC Penney, AutoNation, Gap, Uphold, Levi Strauss & Co., RILA, MGM Resorts, TJX, and Lowe's

ABOUT THREAT INTELLIGENCE

- Trust happens between individuals, not organizations
- Value depends in part on being exclusive
- Channels tend to default to email between individuals

SOCIAL ENGINEERING

- Emphasizing personal connections (in-person meetings, email introductions)

- Never underestimate the power of booze

- People like to be helpful

- Offering frequent reminders of control

- Feedback (appreciation, awards)

Overcoming Barriers to Cybersecurity Threat Intelligence Sharing in the US Retail Sector

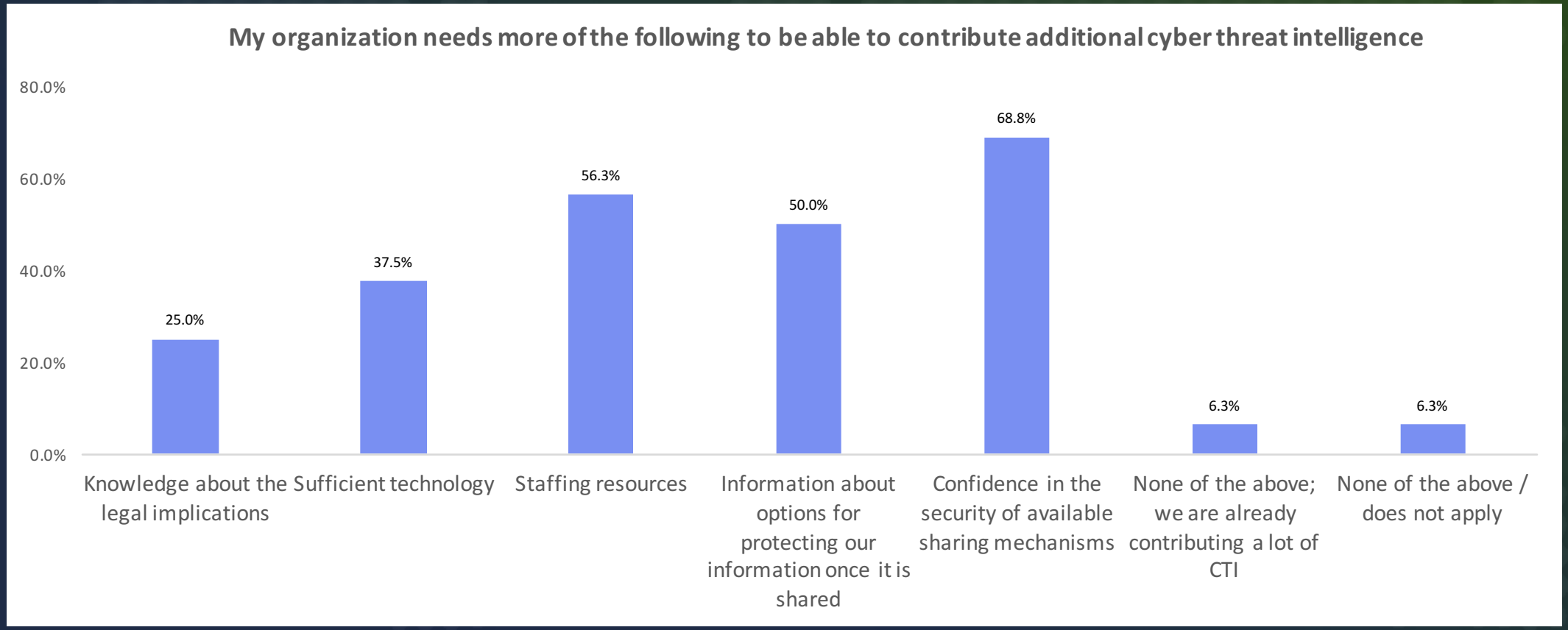
Team One
Kevin Donohue, William MacMillan, Marceia Seabrooks, Mohammed Sorwar

A JOINT RESEARCH PROJECT BY GEORGE MASON UNIVERSITY AND THE RETAIL CYBER INTELLIGENCE SHARING CENTER

GEORGE MASON UNIVERSITY

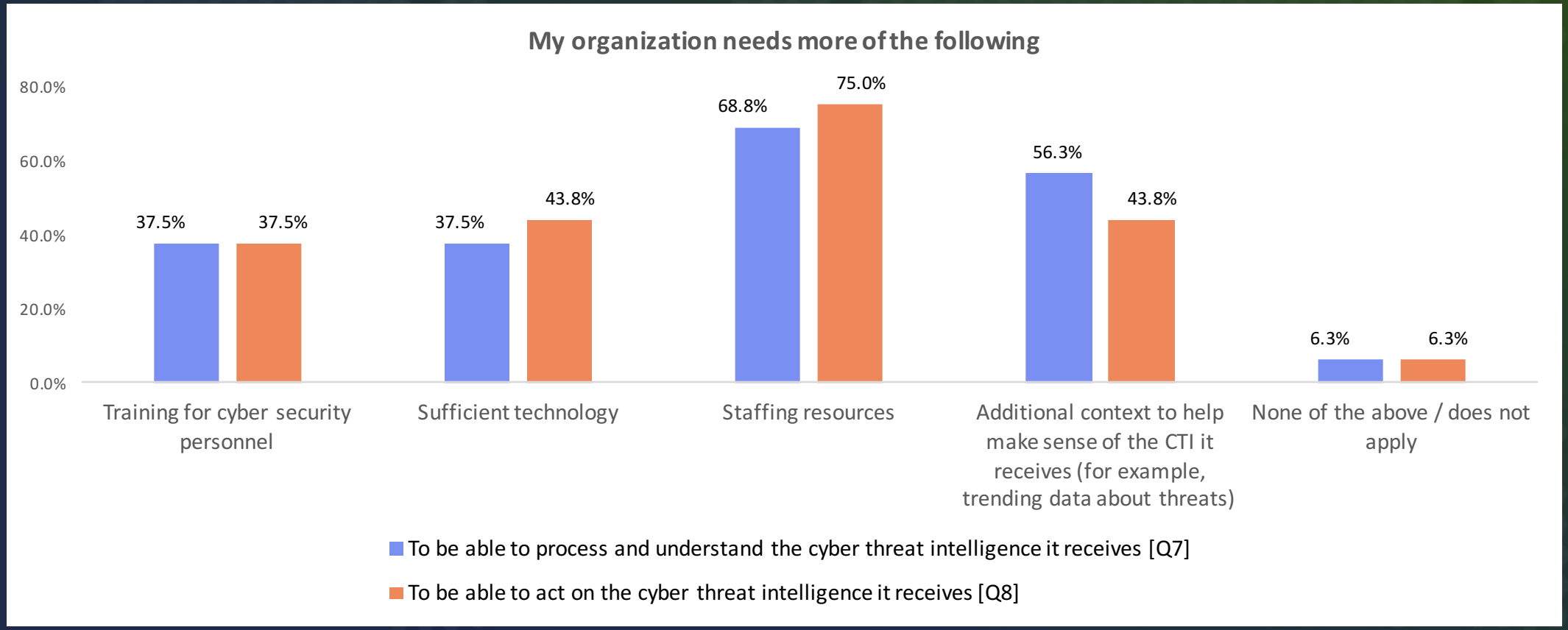
R-CISC RETAIL CYBER INTELLIGENCE SHARING CENTER

FINDING #4: LACK OF CONFIDENCE IN THE SECURITY OF SHARING MECHANISMS IS A BARRIER



R-CISC

FINDING #5: LACK OF STAFFING RESOURCES IS PERCEIVED AS A BARRIER TO THE USE OF CTI

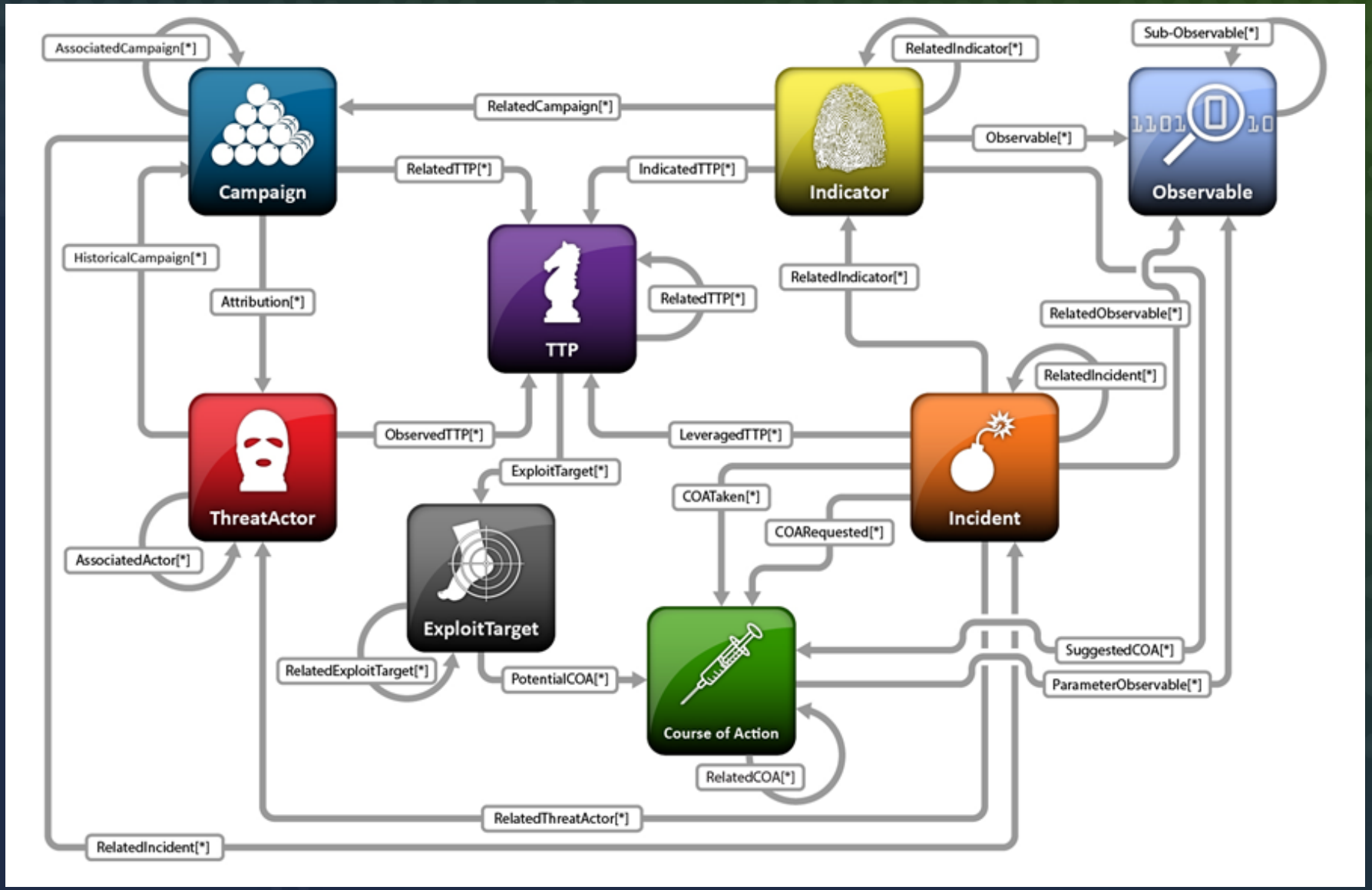


R-CISC

TEMPLATES

TEMPLATES

TEMPLATES


AssociatedCampaign[*]
RelatedIndicator[*]
Sub-Observable[*]
RelatedCampaign[*]
Observable[*]
Campaign
Indicator
Observable
RelatedTTP[*]
IndicatedTTP[*]
HistoricalCampaign[*]
TTP
RelatedTTP[*]
RelatedIndicator[*]
Attribution[*]
RelatedObservable[*]
RelatedIncident[*]
ThreatActor
ObservedTTP[*]
LeveragedTTP[*]
Incident
ExploitTarget[*]
COATaken[*]
COARequested[*]
AssociatedActor[*]
ExploitTarget
SuggestedCOA[*]
RelatedExploitTarget[*]
PotentialCOA[*]
ParameterObservable[*]
Course of Action
RelatedCOA[*]
RelatedThreatActor[*]
RelatedIncident[*]

TEMPLATES

- "Phishing attack"
  - Mail headers
  - Source domains/IPs
  - Time range
  - Where found
  - Email body
  - Target recipients
  - Attachments
  - Impact
  - Kill chain stages
  - Campaign / threat actors

TEMPLATES

- "Phishing attack"
  - Mail headers
  - Source domains/IPs
  - Time range
  - Where found
  - Email body
  - Target recipients
  - Attachments
  - Impact
  - Kill chain stages
  - Campaign / threat actors

{ Anonymous or with attribution?

COMPLICATIONS OF DATA SHARING

- Most are happy to share what they've blocked
- Incidents, not so much (unless they need help from LE)
- Don't want to expose own tools and methods
- Don't want reprisal from adversaries
- Brand reputation trumps liability

HELLO.

TLP: FIFTY SHADES OF AMBER

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

“When we said PEERS, we didn’t mean GOVERNMENT!”

"And we CERTAINLY didn't mean VENDORS!"

COMMERCIAL INTERESTS

- Intellectual property
- Exclusivity
- Marketing
- Sales

UNSTRUCTURED THREAT INTELLIGENCE

THE VELVET ROPE PROBLEM

TECHNOLOGY IS INSUFFICIENT

- Utopia: everything is machine-readable and gets shared at lightning speed, everywhere
- But: not everyone likes STIX/TAXII (sorry)
- And: there are granular concerns around sharing indicators
- By the time you water it down to TLP GREEN, it may be outdated or useless

LESSONS LEARNED FROM THE CYBER-APOCALYPSE

LESSONS LEARNED FROM THE CYBER-APOCALYPSE

- Politics still plays a part, even in / especially in an emergency
- Government doesn't scale

AD HOC NOTIFICATIONS

- Those for whom it comes as a complete surprise
- Those who have a good contact, if only you can find out who it is
- Need secure sharing mechanisms that don't require expertise/technology on both sides
- Keeping OPSEC in place

TAKEAWAYS

- Build up your Rolodex
- Think about multiple communication channels
- Be careful and explicit about sharing restrictions
- Try templates!
- But use whatever works
- Automating your process? Don't forget the sharing stage

R-CISC