
State of the (CTI) Union

Presented by David Eilken



Intro

A silhouette of a hiker wearing a backpack and a beanie, standing on a rocky mountain peak and looking out over a vast, hazy landscape. The hiker is positioned on the left side of the frame, facing right.

Dave

- Architect (Designer of All Things)
- Network Engineer (the IT Guy)
- Arm-Chair Economist (Chicago MBA)
- Start-Up Junkie
- Manager of Big Projects (in China)
- **Cyber Intelligence Sharing**
 - American Express
 - FS-ISAC
 - Soltra



Topics for Discussion

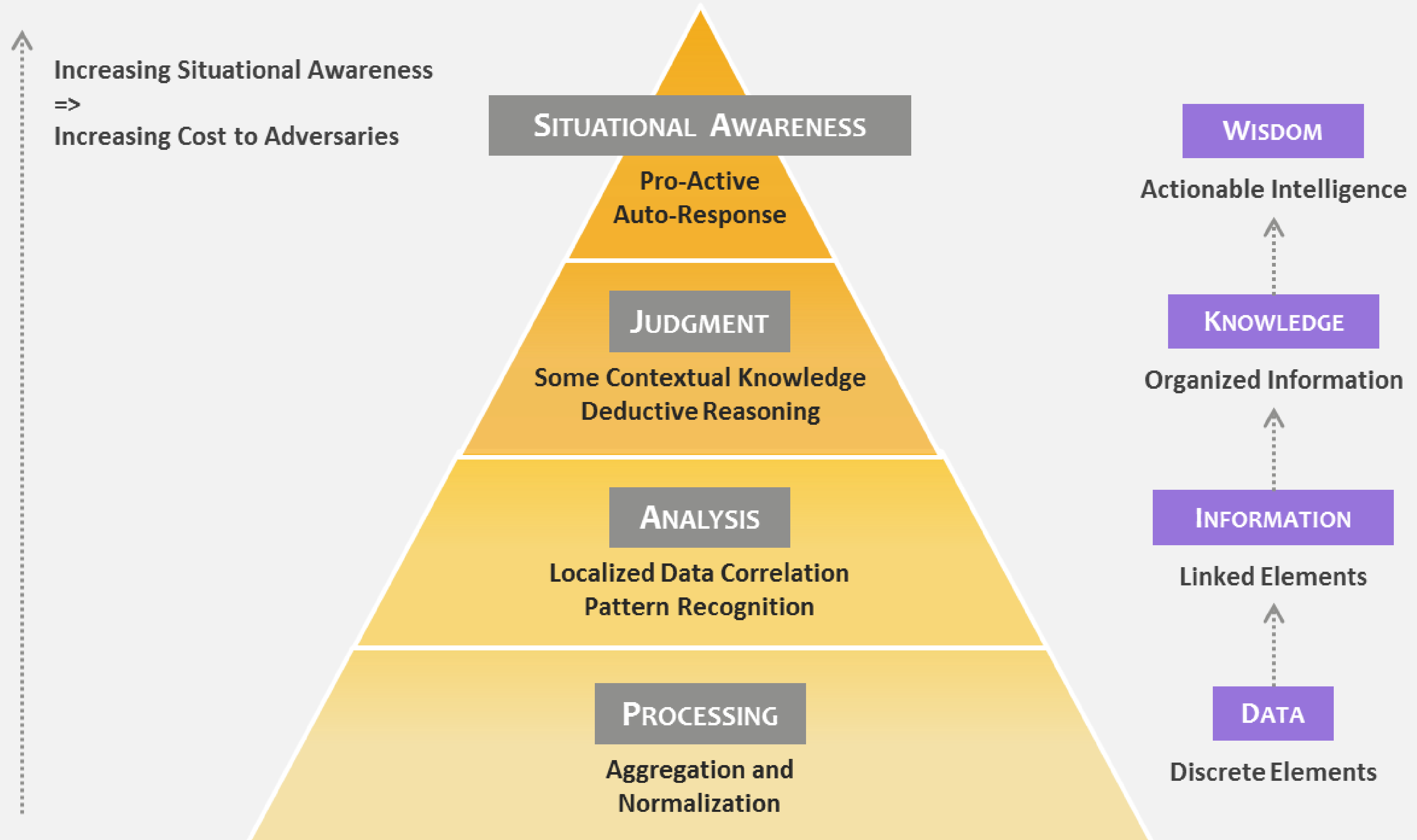
Cyber Threat Intelligence (Sharing)

What, Who, Where, Why
Model for Communities
Challenges
A New Hope
...for the Small & Medium



What is Intelligence?

Levels of Intelligence



High-level definition

Information about a threat



Granular definition

What to look for in your environment to find indication that you have been compromised by a threat.



Examples



A URL to look for used by evil Command and Control:

[[URL: http://mail.googlemailz.com](http://mail.googlemailz.com)]

A file hash of known Malware:

[Hash: d41d8cd98f00b204e9800998ecf8427e]

What is Cyber Intelligence?



Who are the **Industry Players?**

Consumers
(Users & Tools)

Sharing Communities

Producers



Where are we in **time** (and **maturity**)?



THE STATE OF CYBER INTEL

MATURITY

TIME

Early Adopters

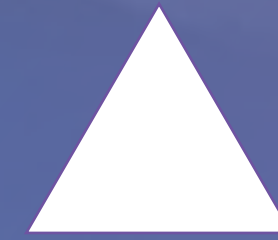
Late Adopters



CTI by ITSELF

Helps Identify Threats

Track
Detect
Respond



CTI when SHARED

Defends as a Group

Distribute to Many
Collaborate
Coordinate Response



Why is CTI Important?



Sharing Communities are at the center.



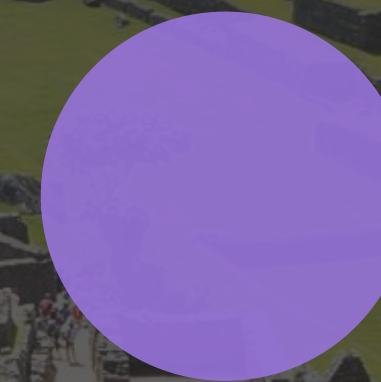
Limitless Options

Sharing communities come in many forms: ISACs, ISAOs, CERTs and private communities



Untapped Potential

We stand to gain even more insight once we learn to use sharing communities to their fullest



Relatability

Members share similar point of view, legal concerns, ways of conducting business, culture



Common Goals

Members share similar priorities for threat defense



Common Needs

Usually organized by industry or interest, making the threat data more relevant than a larger, broader data pool



Rooted in Data

The primary purpose of sharing communities is to share threat intelligence

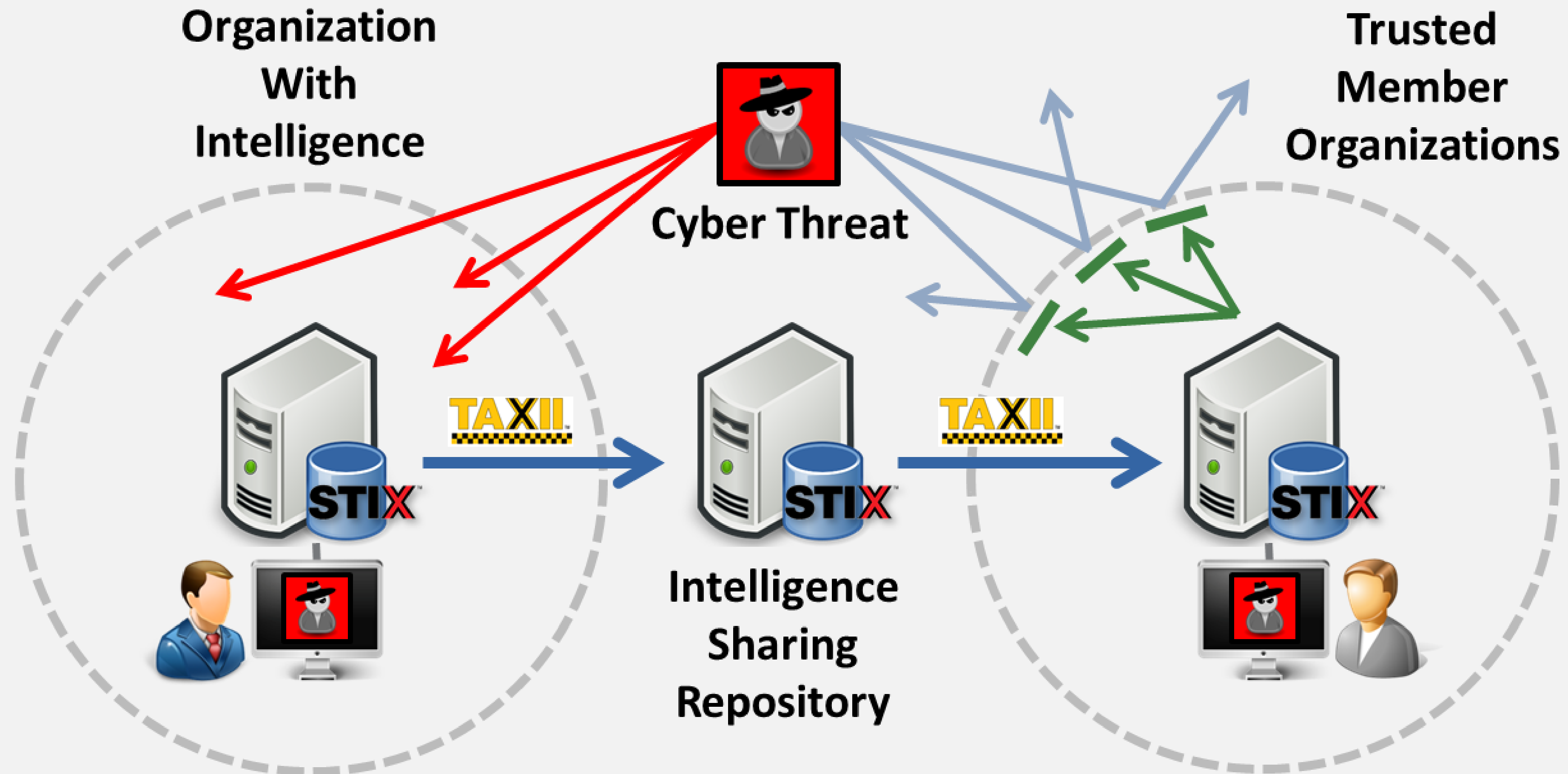


Proposal

A Model for Community Defense



Original Idea



Today We Call These TIPs



Communities face **challenges**

Intelligence Utility

Few organizations protect themselves using the intelligence provided by the community

1

Intel
Utility

Sharing
Back

2

Sharing

Members' inability to participate in the community due to lack of tooling and staffing

Benefits

Member organizations find it difficult to measure community performance and the value to their organization

3

Benefits
As Members



...and have some opportunities

Benchmarking

2

Benchmarking

They could even compare their performance to other organizations through the community

Situational Awareness

1

Situational Awareness

Organizations stand to gain an understanding of which threats are being seen by the community (by both community operators and its members)



Designed over eons, Nature's Defense

Flock
Herd
Swarm
Tribe
Crowd



Meet the Flockers

A **flock** is a group of birds conducting flocking behavior in the midst of flight, or while foraging. The benefits of aggregating in flocks are varied and flocks will form explicitly for specific purposes.

The principal benefits are **safety in numbers** and increased foraging efficiency. **Defense against predators** is particularly important in closed habitats such as forests where predation is often by ambush and early warning provided by **multiple eyes** is important, this has led to the development of many mixed-species feeding flocks.

Flocking also has costs, particularly to **socially subordinate birds**, which are bullied by more dominant birds; birds may also sacrifice feeding efficiency in a flock in order to gain other benefits.

These **multi-species flocks** are usually composed of small numbers of many species, increasing the benefits of numbers but also increasing potential competition for resources.

Advantages

Disadvantages

Sound Familiar?

From Wikipedia, the free encyclopedia



What about **the little guy** (or gal)?

Safety in Numbers
Defense Better

- In Closed Habitats
- Ambushes

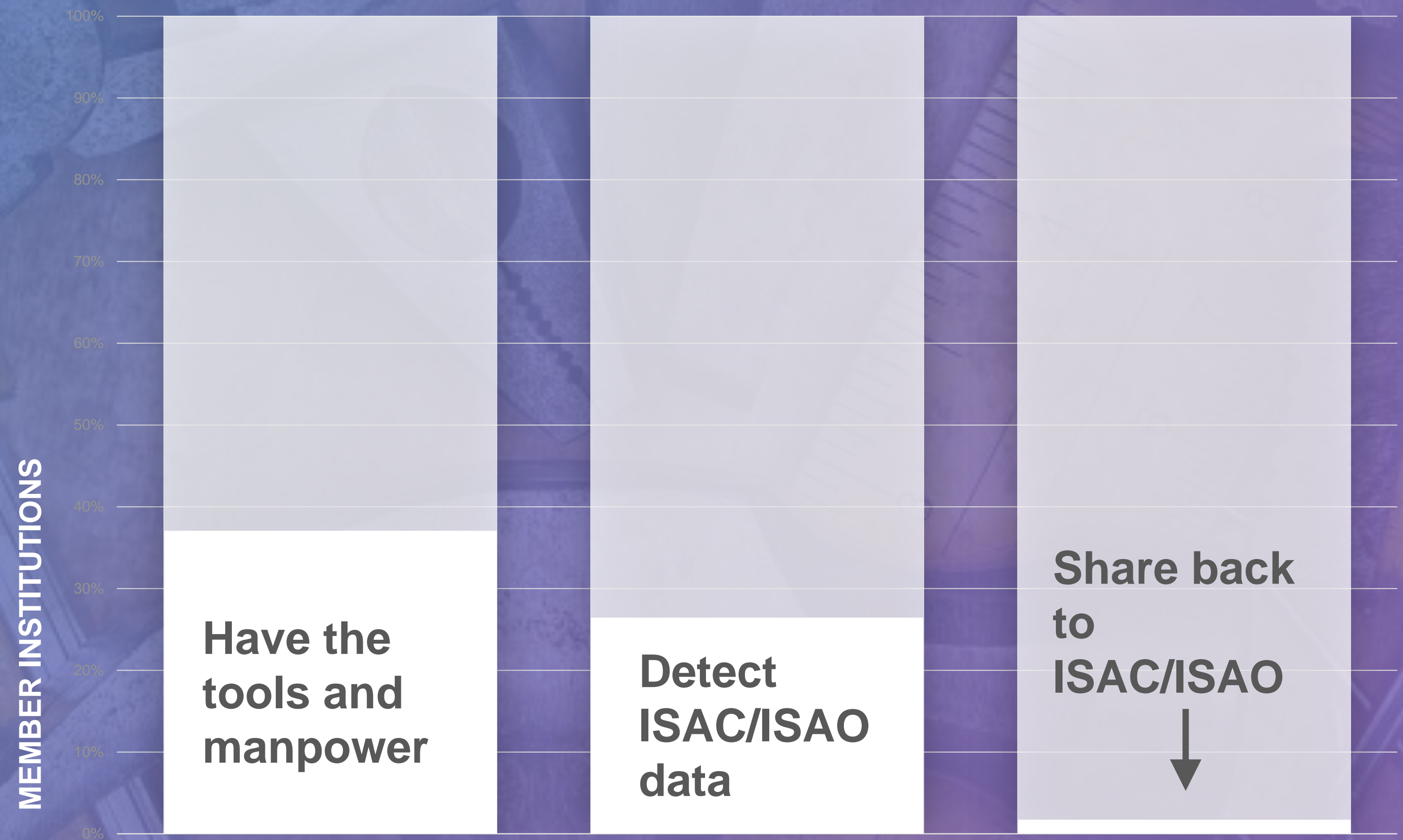
Multiple Eyes

Ignored
Bullied
Sacrificed



**Maturity,
staffing &
tooling**
are holding
us back.

COMMUNITY CYBER INTEL USE



Better **Criteria** for Group Success

Simple

Rules for Individual
Members to Follow
(Easy to Do)

Flexible

Responds Quickly to
Threats
(Covers Many
Situations)

Strong

Resilient to Threats
(Effective)



Are you a **Producer?**

Google & Apple

- Mobile Phone Data

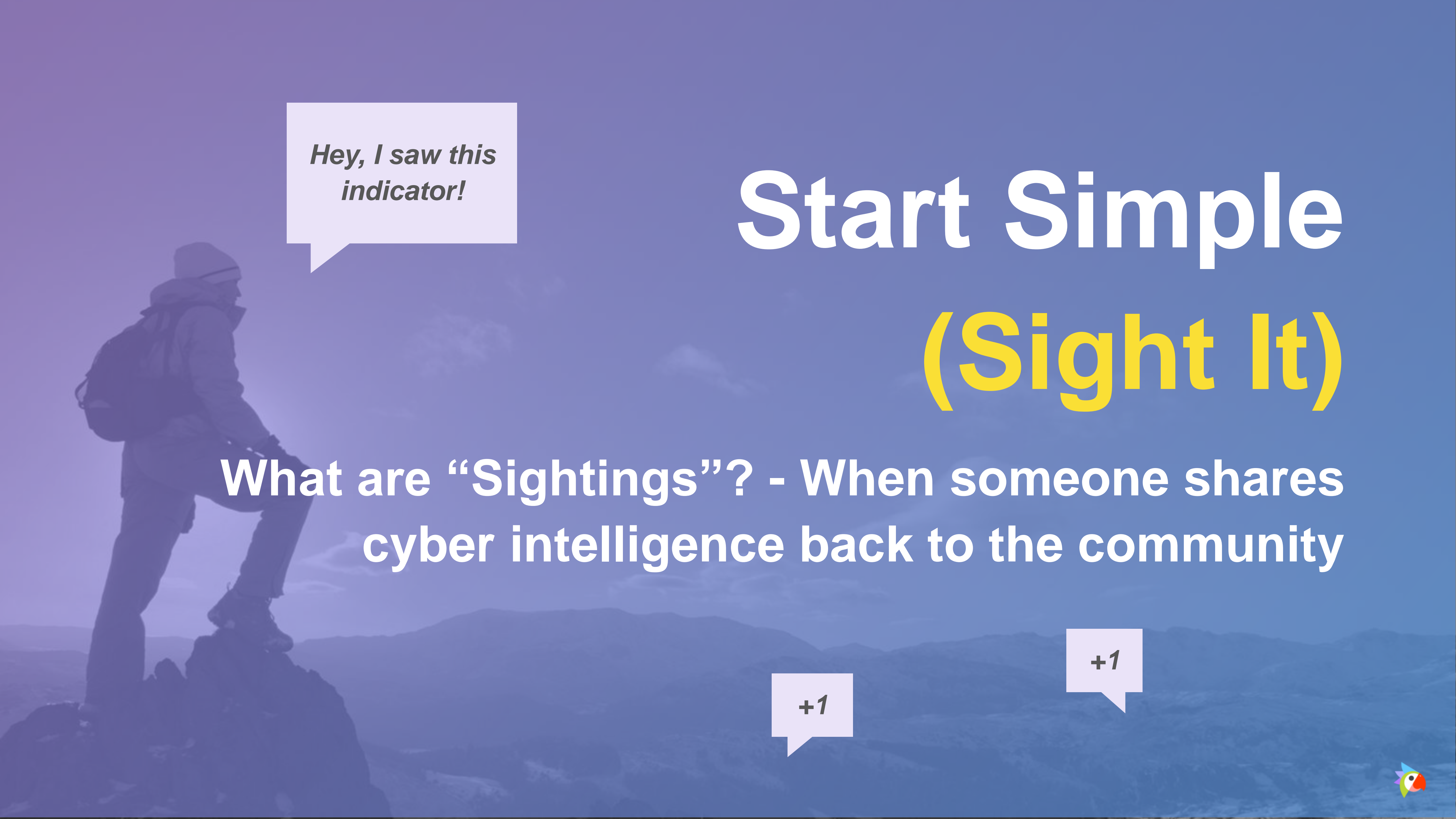
Insurance Companies

- Car Dongle

Monitored

Tethered

Giving Feedback



*Hey, I saw this
indicator!*

Start Simple (Sight It)

What are “Sightings”? - When someone shares
cyber intelligence back to the community

+1

+1



Call to Action

Find Simple Ways To Engage

Share CTI Data (over drinks)

Help Feed the Community

Build Awareness

Support Broad Action

