NORTH TEXAS ISSA

#NTXISSA

Sharing is Real!

Christy Coffey

Business Development Director ISAC/ISAO/Academia

ThreatConnect, Inc.

10/02/2015

What is Threat Intelligence?

In the simplest terms, threat intelligence is the knowledge of a threat's capabilities, infrastructure, motives, goals, and resources.

KNOW YOUR ENEMY!

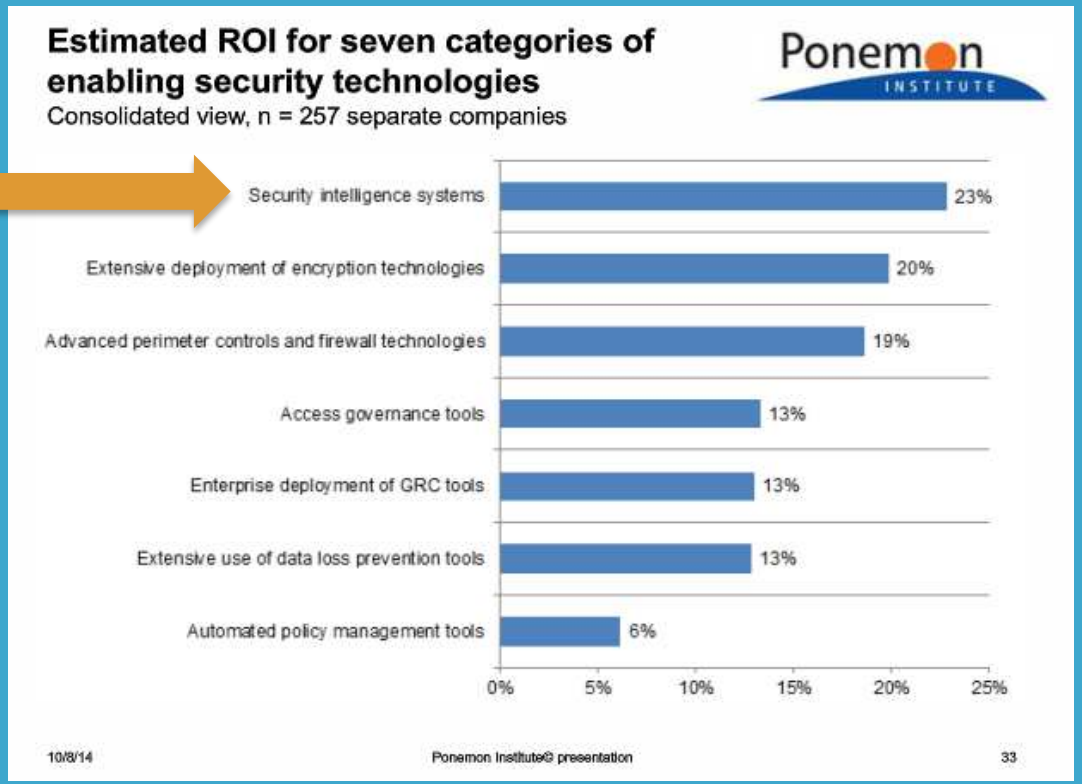
Why do I care?

The application of this information assists in the *operational*, *tactical* and *strategic* defense of network-based assets.

BECAUSE KNOWLEDGE IS POWER

The Need for Threat Intelligence

Average cost of a cyber crime in the U.S. reached **$12.7 million**



Where Does It Come From?

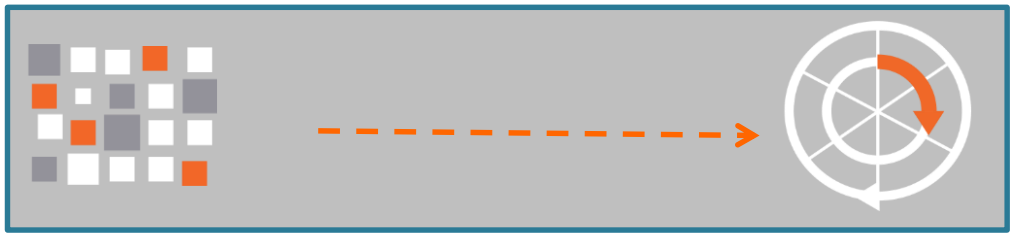
Lots of places…

- Internal Sensors & Research
- Government Feeds & Reports
- Vendor Feeds & Reports
- Open Source (Free) Feeds
- Email Lists & Trust Groups
- Researcher Blogs

Lots of Flavors…

Relevance:

- Type of Threats covered
- Type & Variety of Indicators
  Veracity
- Completeness
- Timeliness
- Structure
- Context

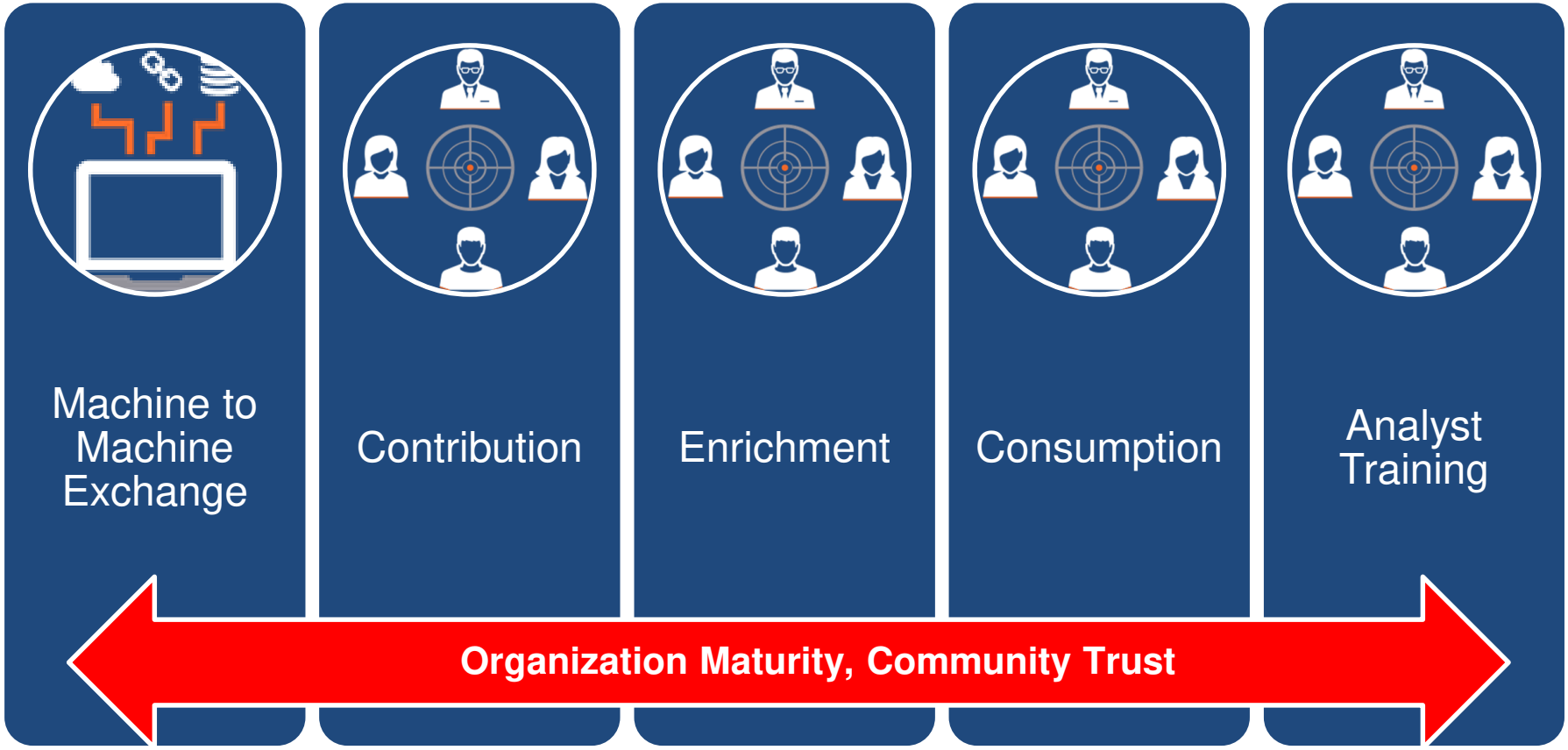


ISACs and ISAOs

Incentives are Emerging to Reward Sharing!

- Council of National Information Sharing and Analysis Centers (ISACs)
  - 17 ISACs
- February 2015: Executive Order 13691 - Promoting Private Sector Cybersecurity Information Sharing
  - Information Sharing and Analysis Organizations (ISAOs)

Sharing Use Cases



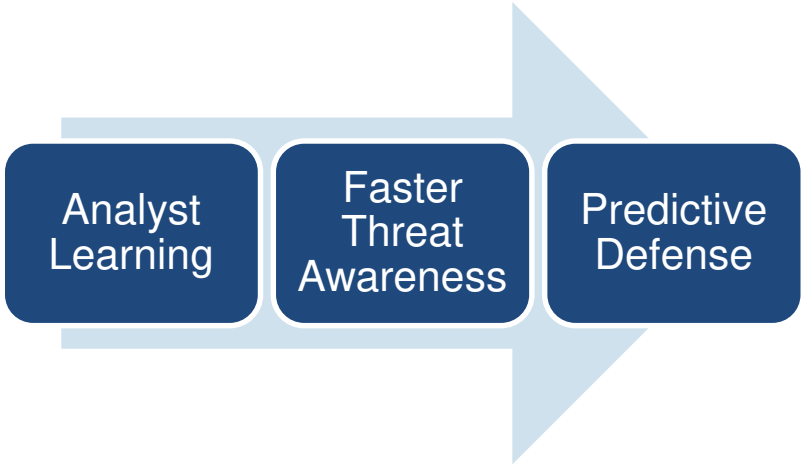
Sharing Success Stories

U.S. Military Organization hosts Community for 5 Mission Partners.

1. Organization 1: Contributes 50 indicators
2. Organization 3: Provides a related spear phish
3. Organization 5: Finds active infection
4. Organization 2: Finds Organizations 5's malware in repository from previous incidents.

Company is targeted by an APT group multiple times across 2 year span.

Community tip provides valuable insight, and enables company to put protective defenses in place to block APT for the first time.



Advice from NIST

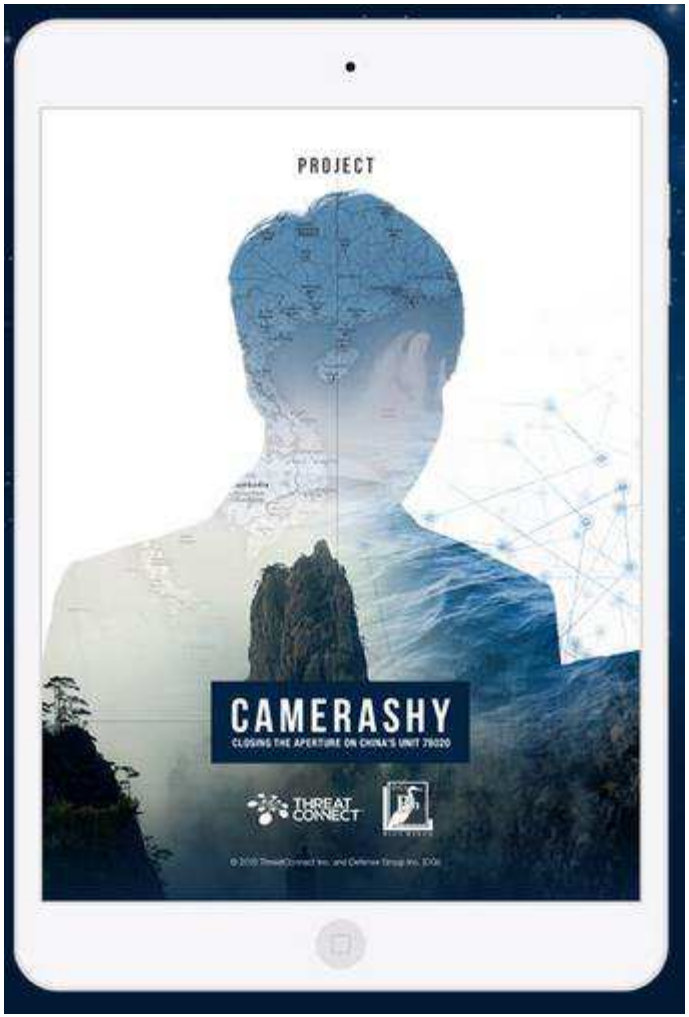
"Cyber Security: Your Mother Was Right, Sharing is Good, And NIST Has Some Help on How"

"An organization should move from an informal, ad hoc, reactive cyber security approaches" (p.19)

"Establish information sharing rules" and "Joining a sharing Community" are important first steps (p.27)

NIST 800-150: "Guide to Cyber Threat Information Sharing"

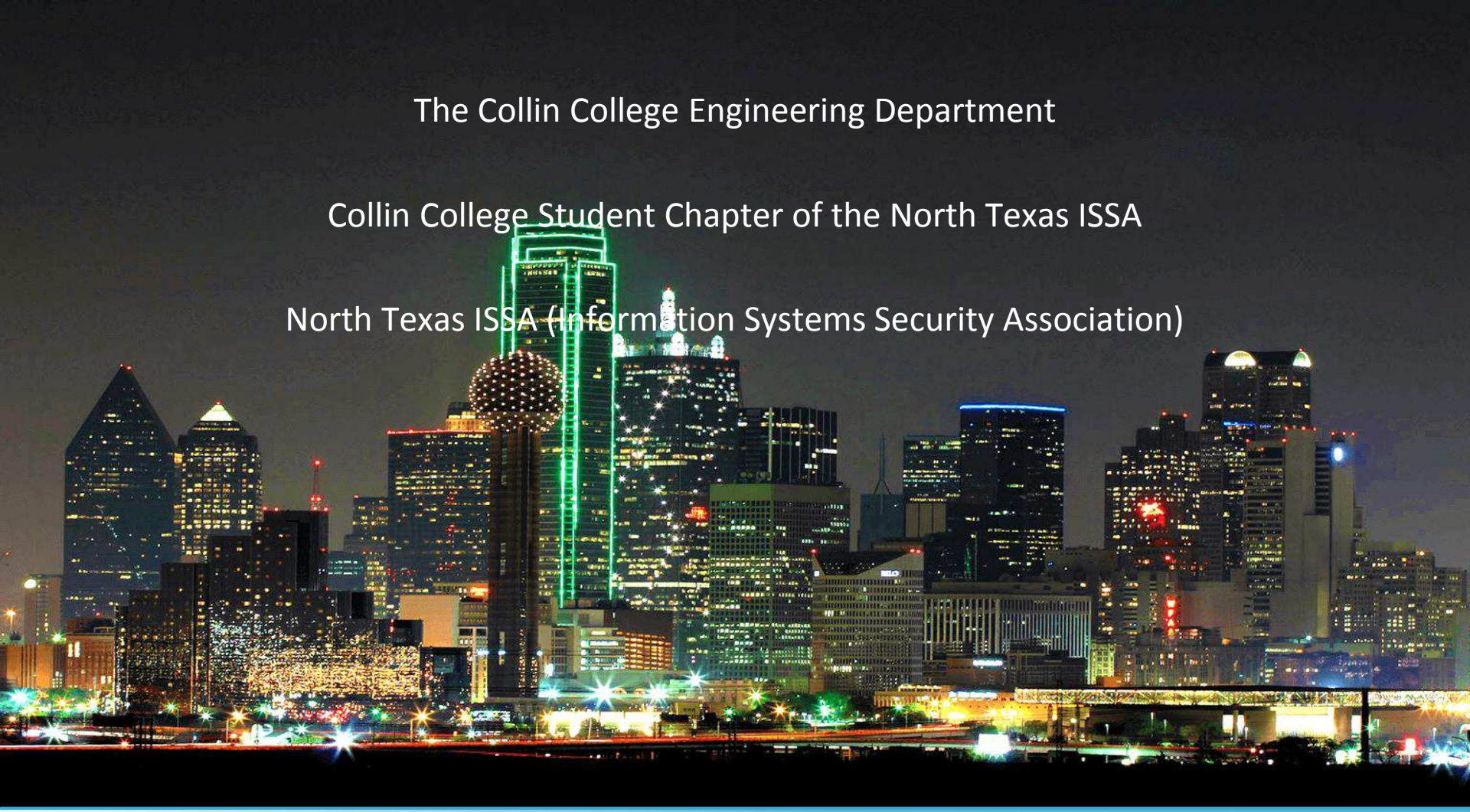
Get Started!



- Open Source Data
- Free Communities
- Threat Intelligence Platforms

References

- National Council of ISACs -> here
- Executive Order 13691 - Promoting Private Sector Cybersecurity Information Sharing -> here
- NIST 800-150 “Guide to Cyber Threat Information Sharing” -> here
- ThreatConnect -> here
- Community Collaboration Case Study -> here
- Operation CameraShy -> here


The Collin College Engineering Department
Collin College Student Chapter of the North Texas ISSA
North Texas ISSA (Information Systems Security Association)

Thank you