How enterprises can use cyber threat information effectively?

Shimon Modi, Ph.D.
smodi@trustar.co
@shimonmodi

About Me

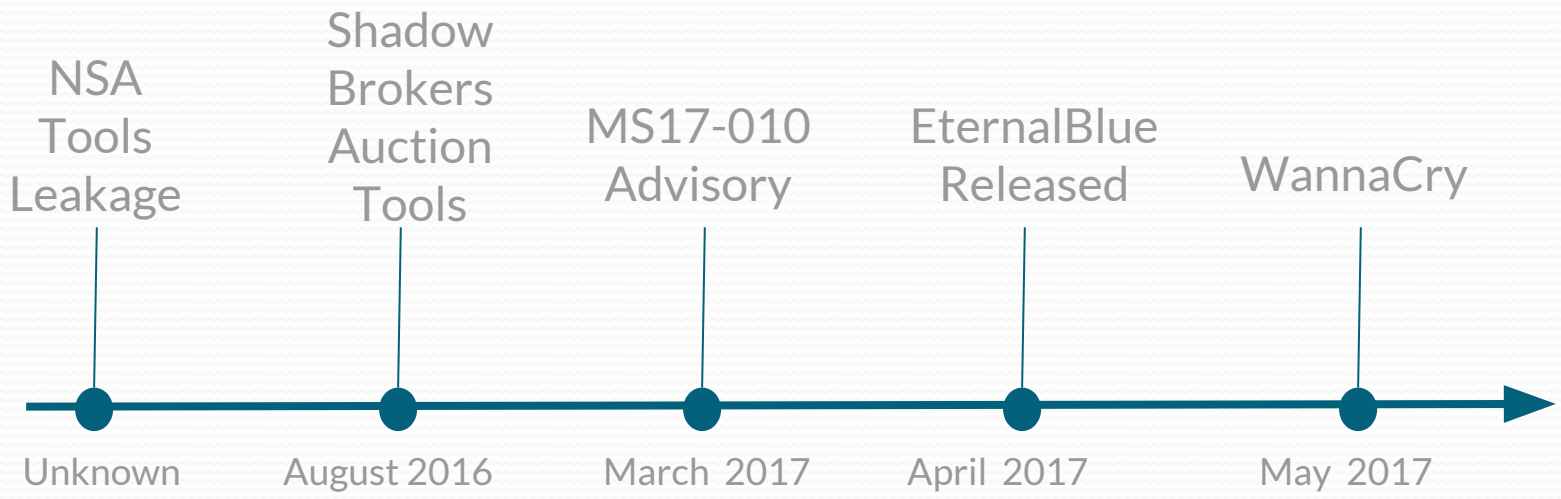
- 10+ years of Applied R&D experience in Information Security
- Currently @ TruSTAR Technology - Head of Product
- Previously @
  - Accenture Technology Labs - Cyber R&D team
  - Director of Research, Biometrics Lab at Purdue University
- Ph.D. - Purdue University
  - Authored book on “Biometrics & Identity Management” for security professionals

Agenda

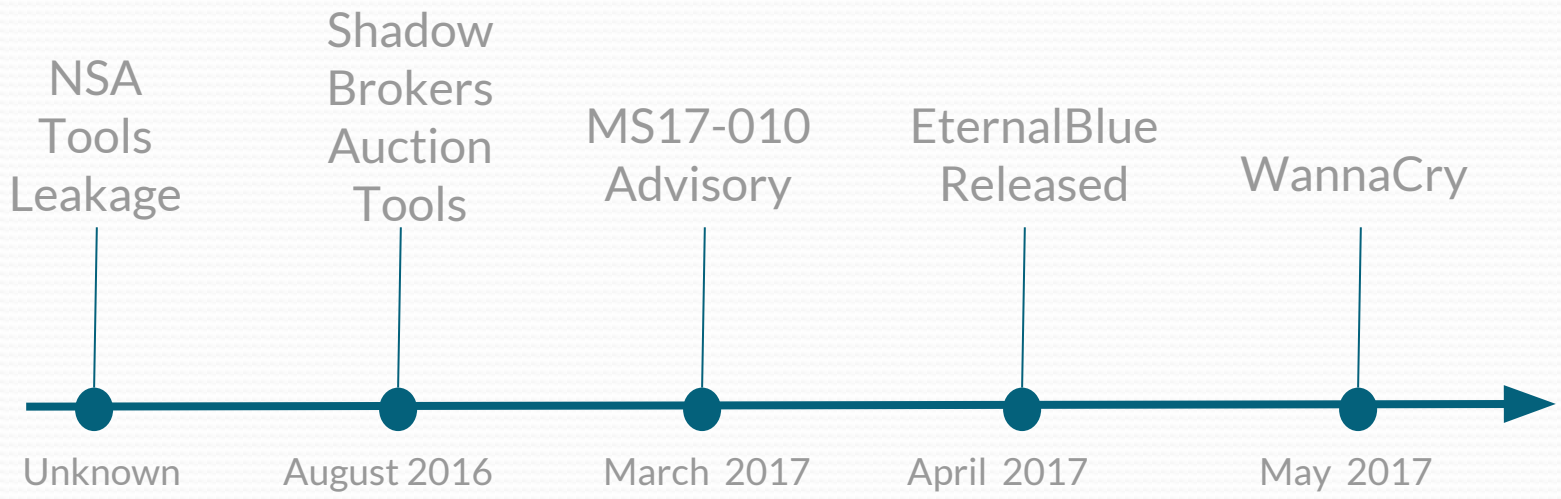
- Framing the Topic
- Charting Your Journey
- Challenges (& Solutions)
- Taking the First Step

Root this in reality...

Putting things in perspective: WannaCry



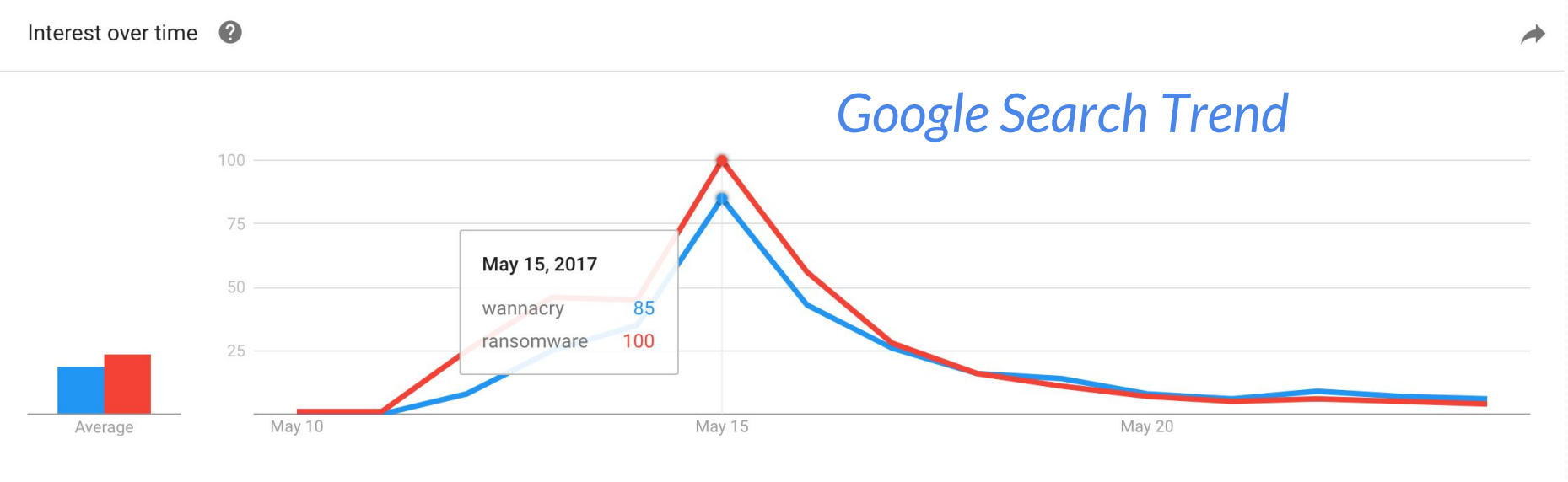
Putting things in perspective: WannaCry



And this happened next...

Lots of (ad-hoc) activity

Lots of (ad-hoc) activity



Driven by **3 motivating factors**:

- Gather all IoC's you can
- See if anyone has published actionable information
- Reduce uncertainty in own understanding of the attack

Cyber Threat Intelligence (CTI) is the Answer!!

So..what is CTI?

Is it a data feed? ✖

A threat intelligence program should be more than feeds with no context and actionability. Threat feeds form an integral part of any threat intelligence program but it cannot standalone as a comprehensive solution.

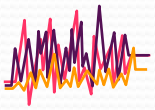
Is it a replacement for security operations? ✖

Threat intelligence should supplement your security operations. Threat intelligence should be integrated into daily operations, amplifying the effectiveness of traditional security mechanisms.

CTI should help...

Understand cyber activity that is being observed

Prioritize threats and vulnerabilities that need to monitored



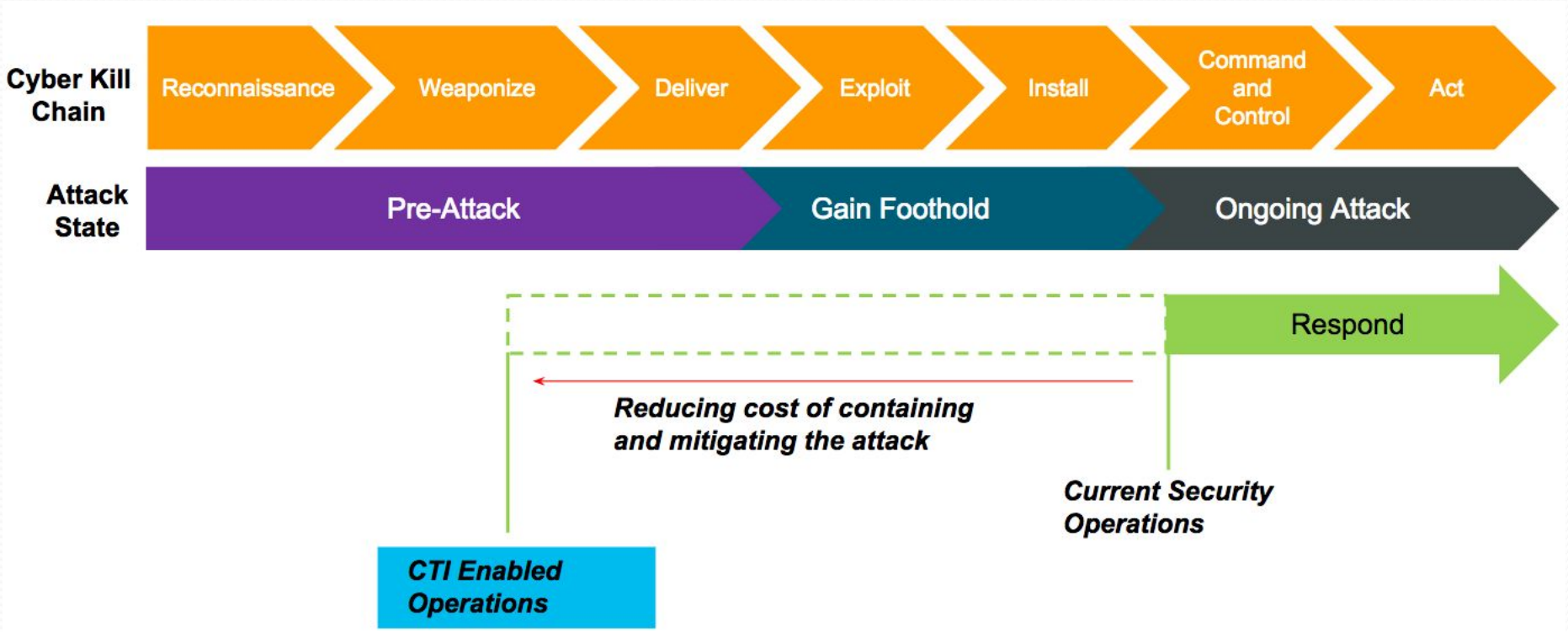
Gain a historical perspective of threat activity

Comprehend how attacker makes their moves.

Understand motives of the threat actor

Determine mitigation action, either proactive or reactive, against threat activity

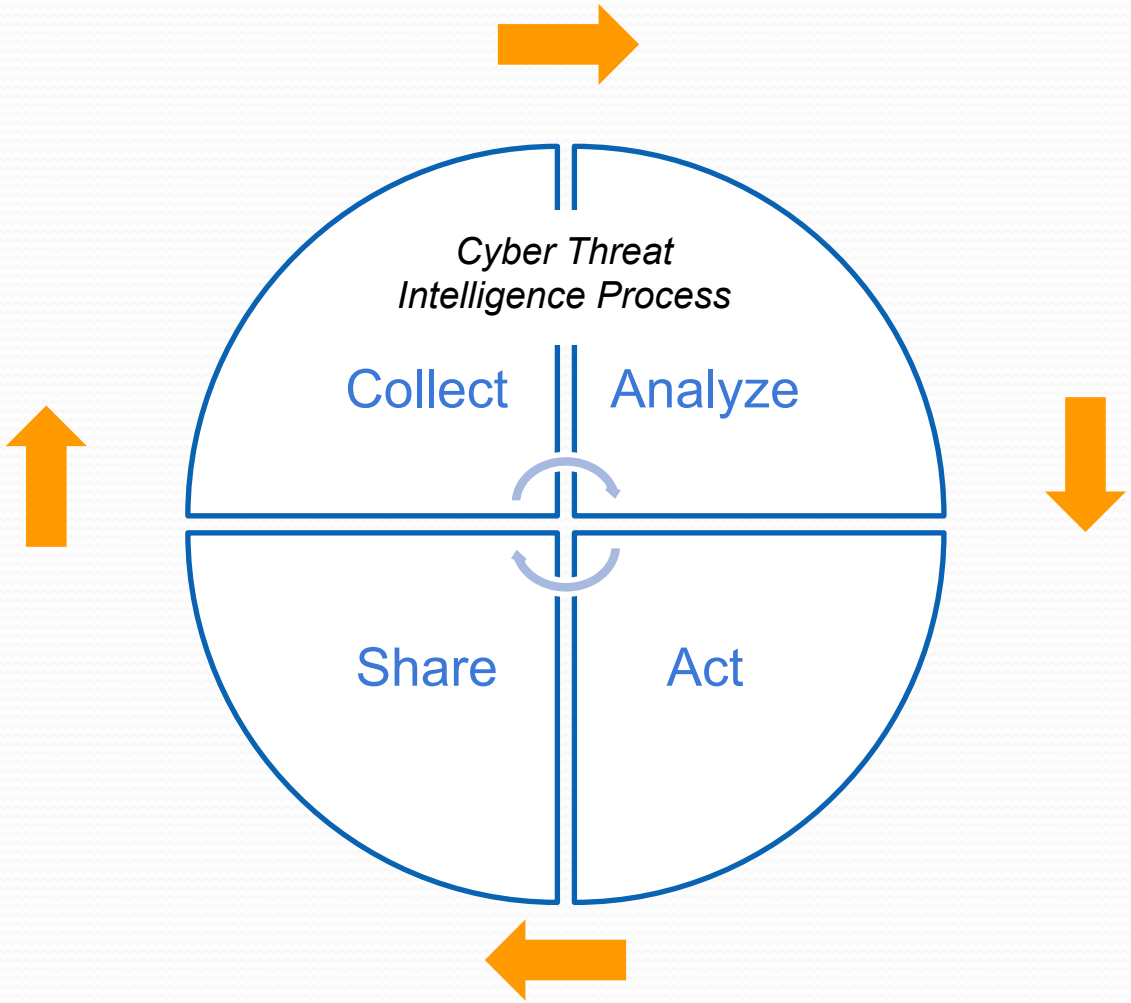
Outcome



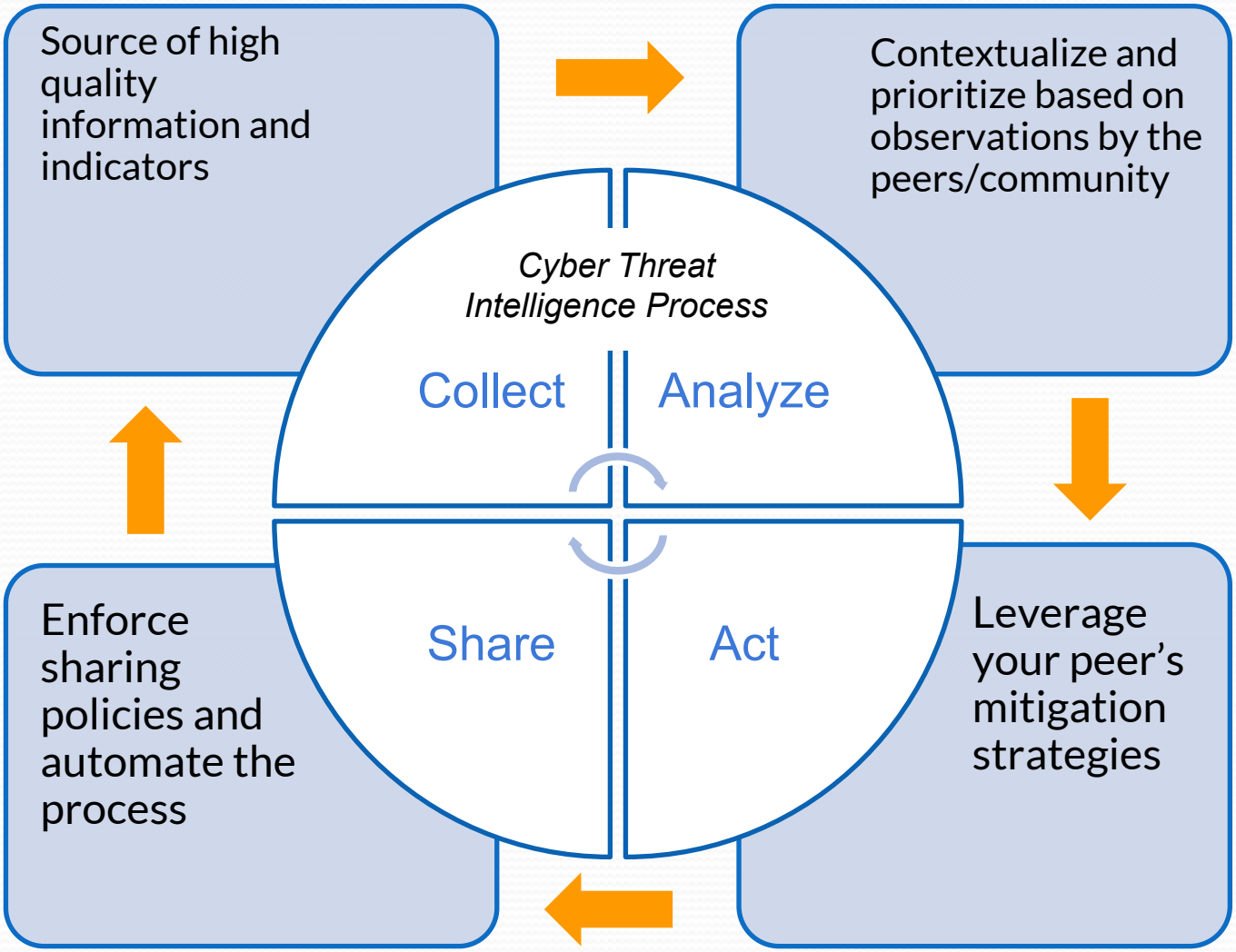
Change Economic Dynamics to Favor Defenders

Charting Your Journey

CTI Process


Cyber Threat
Intelligence Process
Collect
Analyze
Share
Act

CTI + Intelligence Exchange



Some Basic Challenges

Challenges

1. Information is available in a number of different formats and requires transformation to make it usable
2. Varying quality of threat information slows down internal processes
3. Time is important - SOC/ IR processes need to access to the most relevant information

Challenge & Solution(s)

1. Information is available in a number of different formats and requires transformation to make it usable

2. Varying quality of threat information being shared and exchanged slows down internal processes

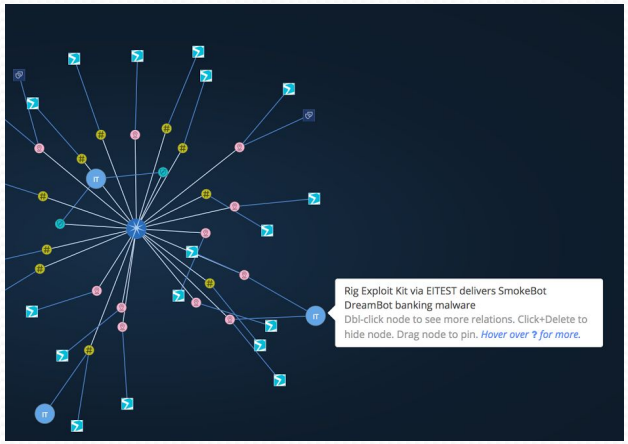
3. Time is important - SOC/ IR processes need to share and have access to shared information quickly

NIST Special Publication 800-150

Guide to Cyber Threat Information Sharing

June 20, 2017 – Issues that Matter: Protecting the Enterprise

Threat Intelligence Platforms



Journey of Thousand Miles Starts with a Step

Start with Quick Wins

External Data Feeds

Curated List of Resources & Tools:
https://github.com/hslatman/awesome-threat-intelligence

Start with Quick Wins

External Data Feeds → Move Towards Enrichment

Curated List of Resources & Tools:
https://github.com/hslatman/awesome-threat-intelligence

Start with Quick Wins

External Data Feeds → Move Towards Enrichment → Correlation / Event Manager

Curated List of Resources & Tools:
https://github.com/hslatman/awesome-threat-intelligence

Key Takeaways

1. Use CTI to support all cybersecurity and risk management processes

2. Start by operationalizing internally and then expand into external exchange

3. Join a sharing community and start connecting with peers

Thank You!

Contact Information: smodi@trustar.co
Twitter: @shimonmodi