RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Using Automated Cyber Threat Exchange to Turn the Tide against DDOS

SESSION ID: ANF-R01

Moderator: Dr. Peter Fonash
Chief Technology Officer, Cybersecurity & Communications
US Department of Homeland Security

Panelists: Dr. Phyllis Schneck
Deputy Undersecretary for Cybersecurity
US Department of Homeland Security

Joe Demarest
Assistant Director, Cyber Division
Federal Bureau of Investigation

Mark Clancy
Managing director of Technology Risk Management,
Depository Trust & Clearing Corporation

Richard Struse
Chief Advanced Technology Officer, NCCIC
US Department of Homeland Security

Our Goal:

Create an ecosystem where actionable cyber threat intelligence is automatically shared in real-time enabling real-time defense - the detection, prevention and mitigation of cyber threats such as DDOS before or as they occur

Presenter's Company Logo – replace on master slide

“Automated”

- Leverage machines to perform routine and tedious tasks
- Free humans to perform analysis and exercise discretion

“Cyber Threat Intelligence”

- What activity are we seeing?
- What threats should I look for?
- Where has this threat been seen?
- What does it do?
- What weaknesses does it exploit?
- Why does it do this?
- Who is responsible for this threat?
- What can I do about it?

Presenter’s Company Logo – replace on master slide

Barriers to Real-time Intelligence

- No standardized language for cyber threat information
- Can vary widely in terms of:
  - Transmission formats
  - Levels of abstraction
  - Degrees of structure
- Difficult to ensure consistent interpretation
- Challenging to automate

Reports

Email

```
10.6.2.34
,TCP,80,0
7:21:22.0
3
```

CSV

Presenter's Company Logo – replace on master slide

Discussion and Q & A

Backup Slides

But what does
“Automated Cyber Threat Intelligence Sharing”
really mean?

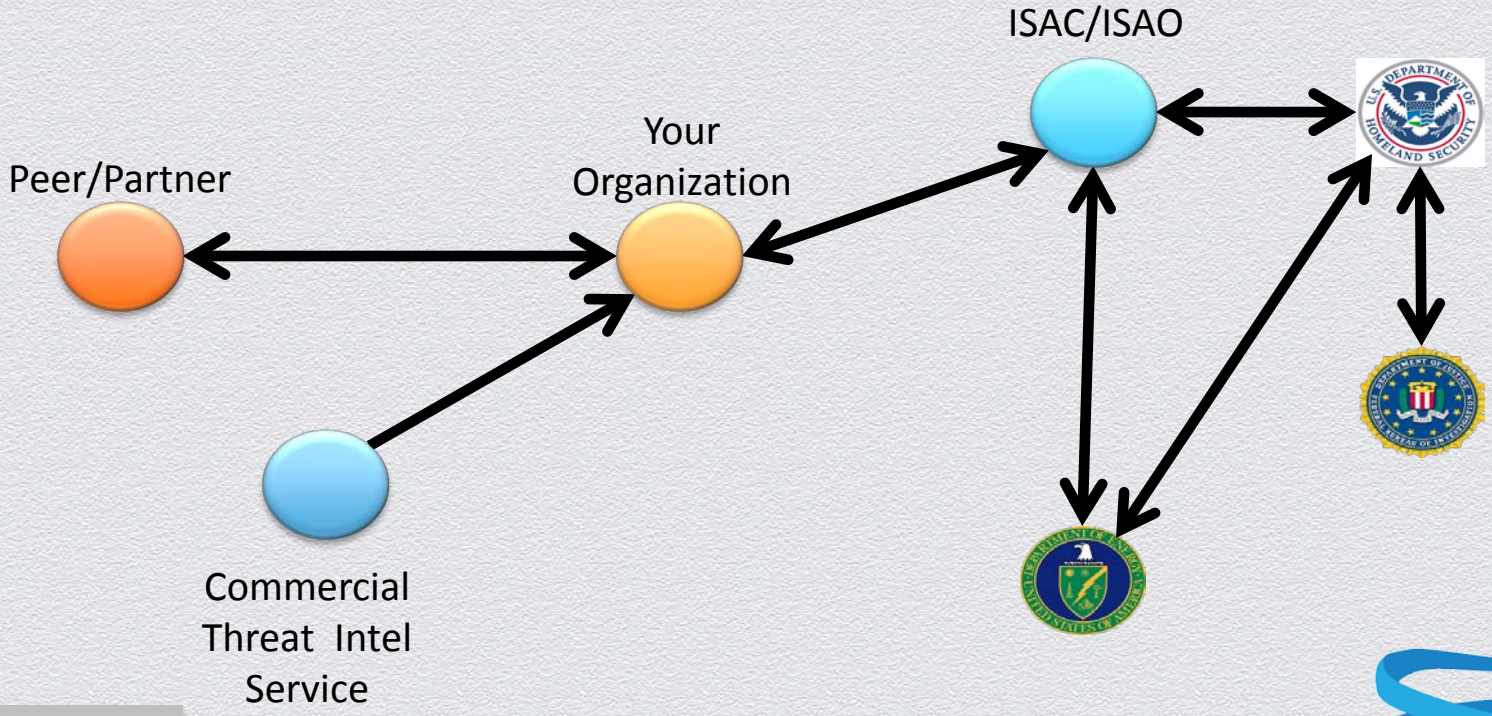
Presenter’s Company Logo
– replace on master slide

Sharing

- Sharing information about cyber threats with your sector, partners and others
- Voluntary exchange of appropriately anonymized indicators and other threat data
- Leveraging existing communities of trust
- You choose what to share
- You choose whom to share with

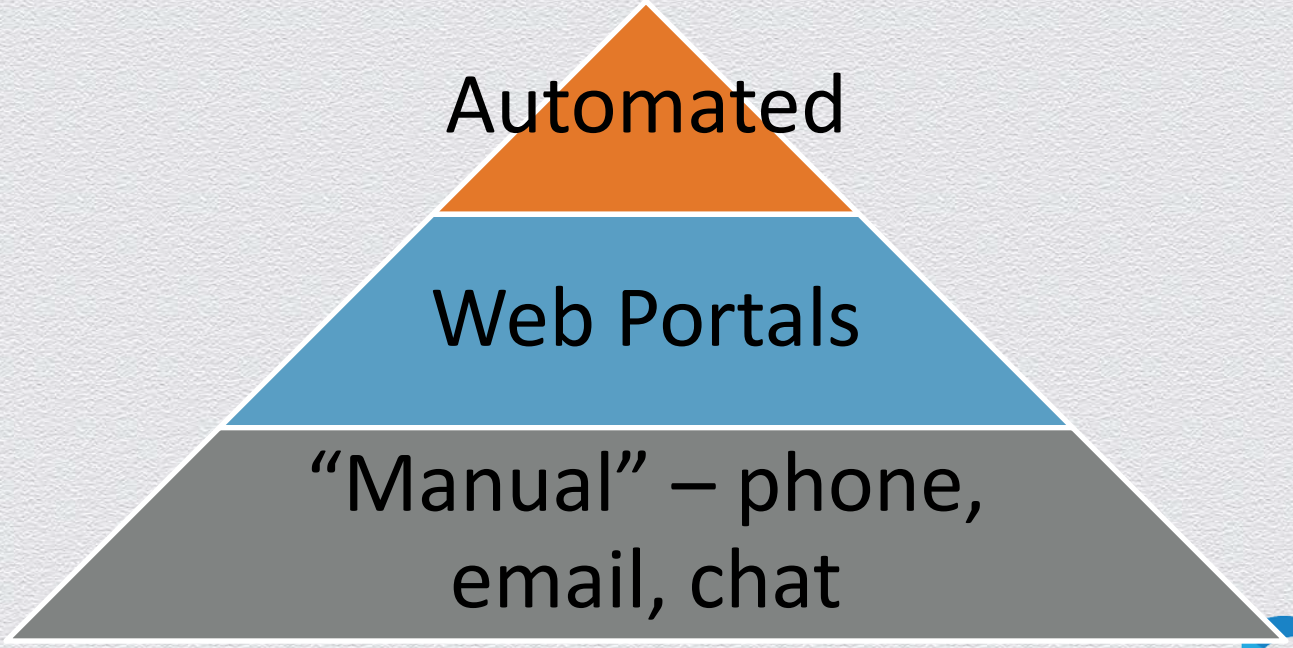
Presenter's Company Logo – replace on master slide

Notional Cyber Indicator Sharing Ecosystem



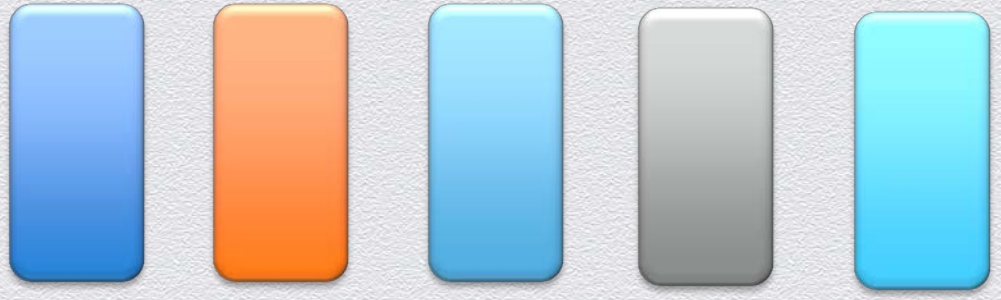
Presenter's Company Logo – replace on master slide

Current Cyber Threat Intelligence Sharing Methods

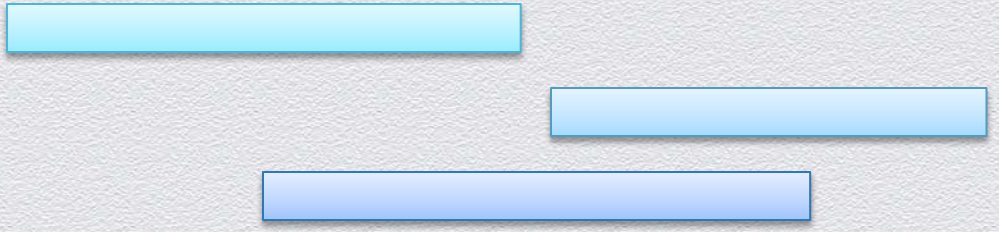


Presenter’s Company Logo – replace on master slide

Bridging the Gaps



Organizations / Sectors



Sharing Communities / Programs / Services

Common Format & Transport

STIX TAXII

Presenter's Company Logo – replace on master slide