Cyber-Threat Intelligence Sharing –

Speeding up Incident Response

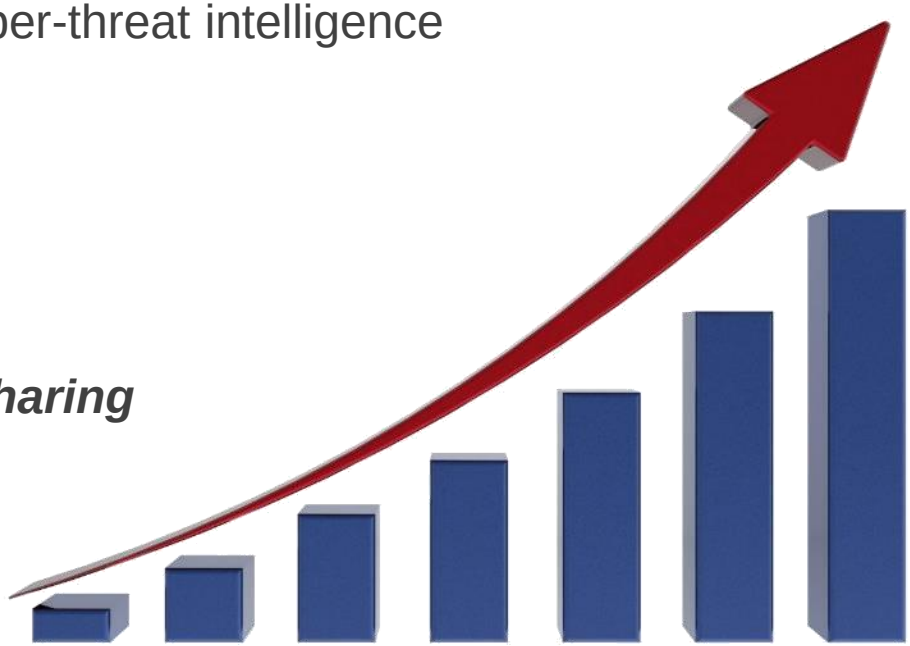
X-Congress
Bogotá, Colombia – Oct. 2016

Financial Services ISAC

A Brief Overview

- Nonprofit private sector initiative since 1999
- Designed/developed/owned by financial services industry
- Sharing information globally (members in ~40 countries w/ a user base in >70 countries)
- Risk reduction through sharing cyber-threat intelligence
- Ca. 7,000 members worldwide

➢ ***Enabling security information sharing and collaboration at all levels***



FINANCIAL SERVICES ISAC

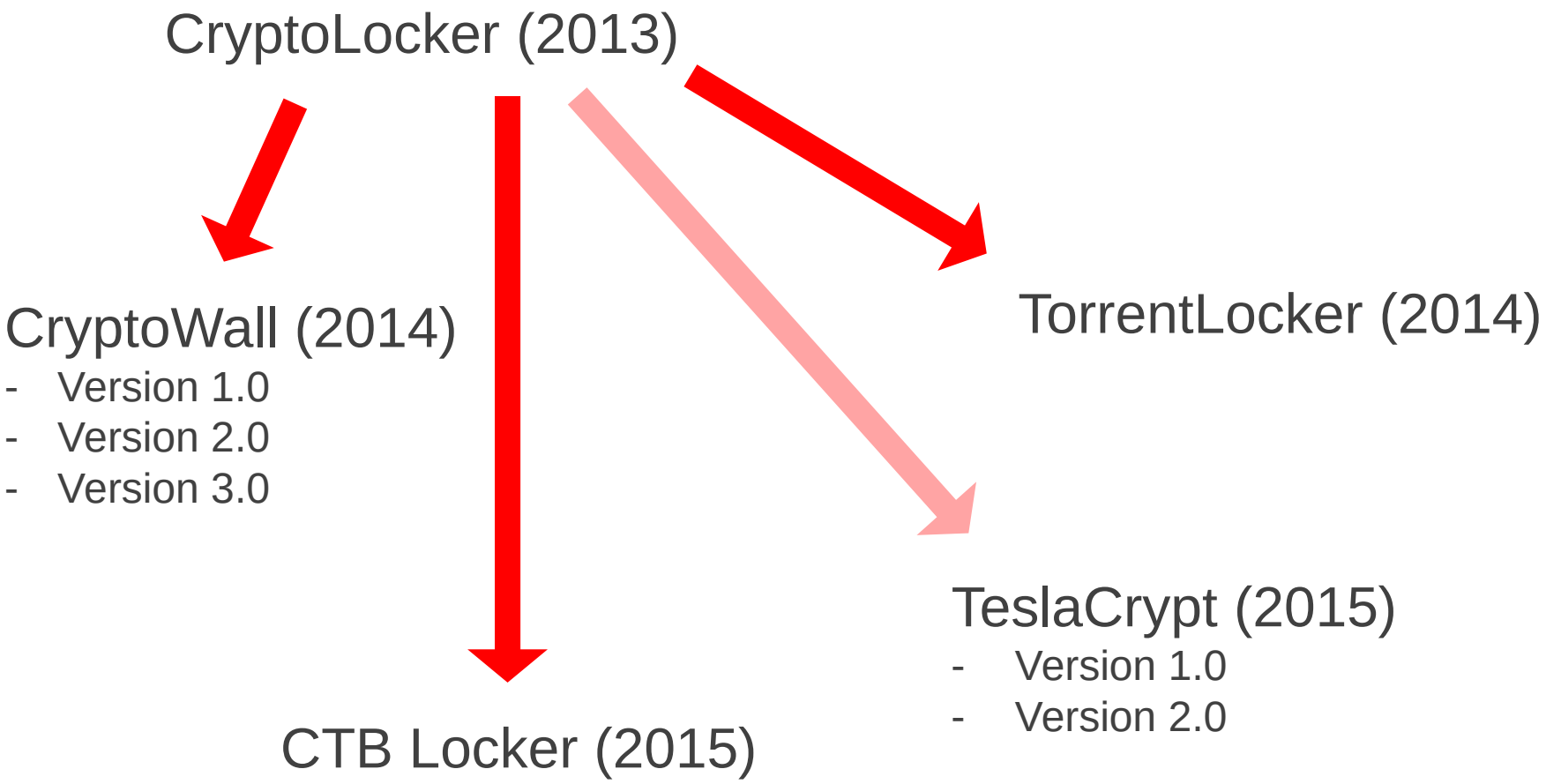
 © 2016 FS-ISAC

Threats Spread Globally

E.g. Retefe Banking Trojan

 © 2016 FS-ISAC

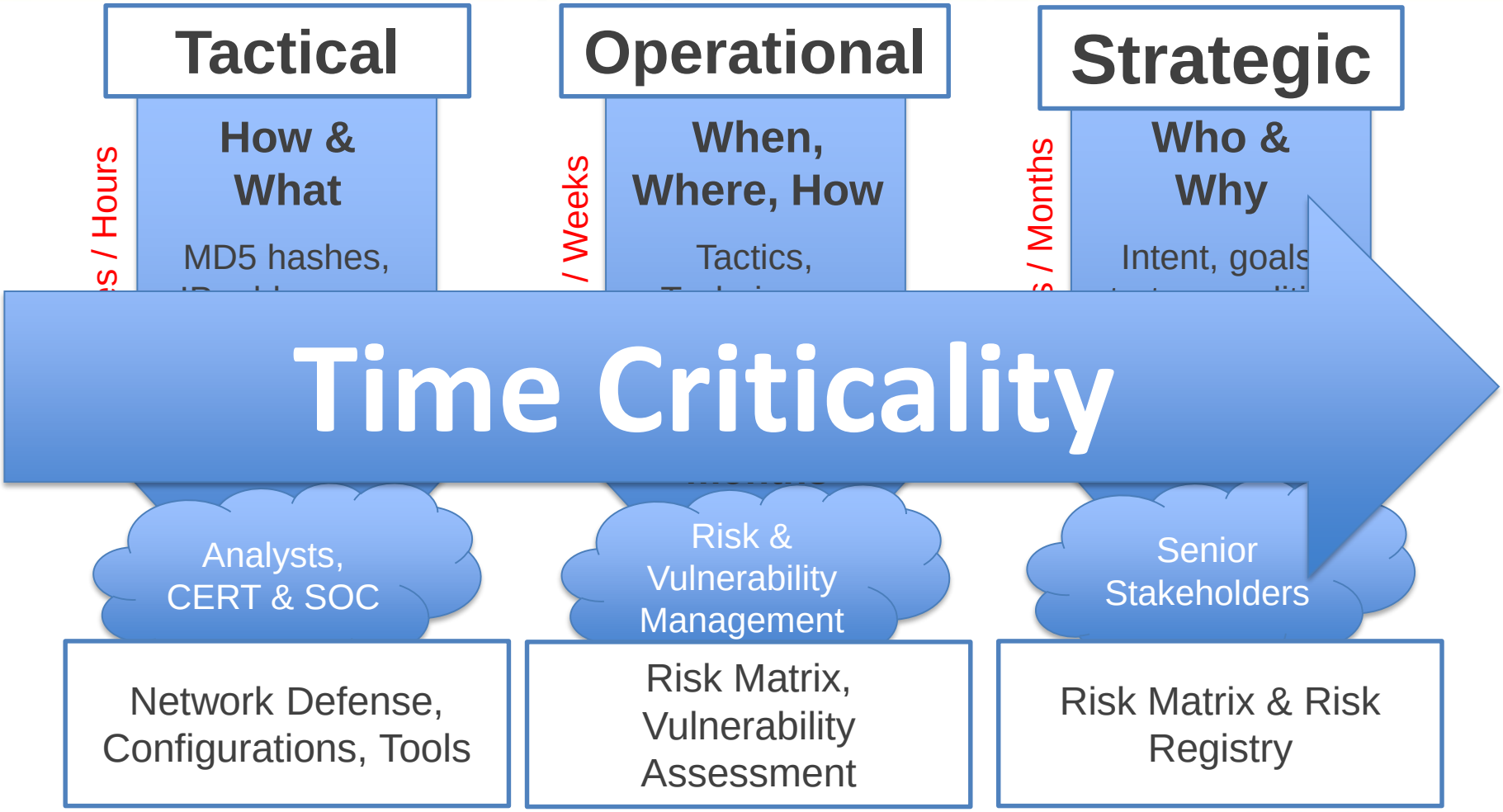
Threats Evolve over Time



 © 2016 FS-ISAC

Timeline of Security Information

Types of Relevant Information



The Need for Info Sharing is Increasing

No Financial Firm is Capable of Facing all Threats Alone

Increasing Attack Volume, Complexity

Rising Breach Costs

Growing Regulatory Pressures

Exploding Threat Indicator "Noise"


Cost of a data breach: 58 cents per record, says Verizon


CRAIN'S NEW YORK BUSINESS

DATA & LISTS VIDEO NEWSLETTERS CUSTOM CONTENT TV

Health Care Politics Technology More Industries

ancing the weight of big decisions?

The insight you need to make decisions of impact

Deloitte Growth Enterprise Services

ybersecurity costs doubling

ar on computer security, was recently hacked.


BRIEFING ROOM ISSUES THE ADMINISTRATION

The White House

Office of the Press Secretary

For Immediate Release

FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing


1,554

Number of installations of FS-ISAC's Soltra Edge information-exchange platform in the first four months after it was launched Dec. 3

12 million

Number of threat indicators in FS-ISAC's cyberthreat repository as of Oct. 1, a fivefold increase from a year earlier

10,000+

Number of daily manual

FINANCIAL SERVICES ISAC

TLP Green

The Incident Response Process

Before -> During -> After

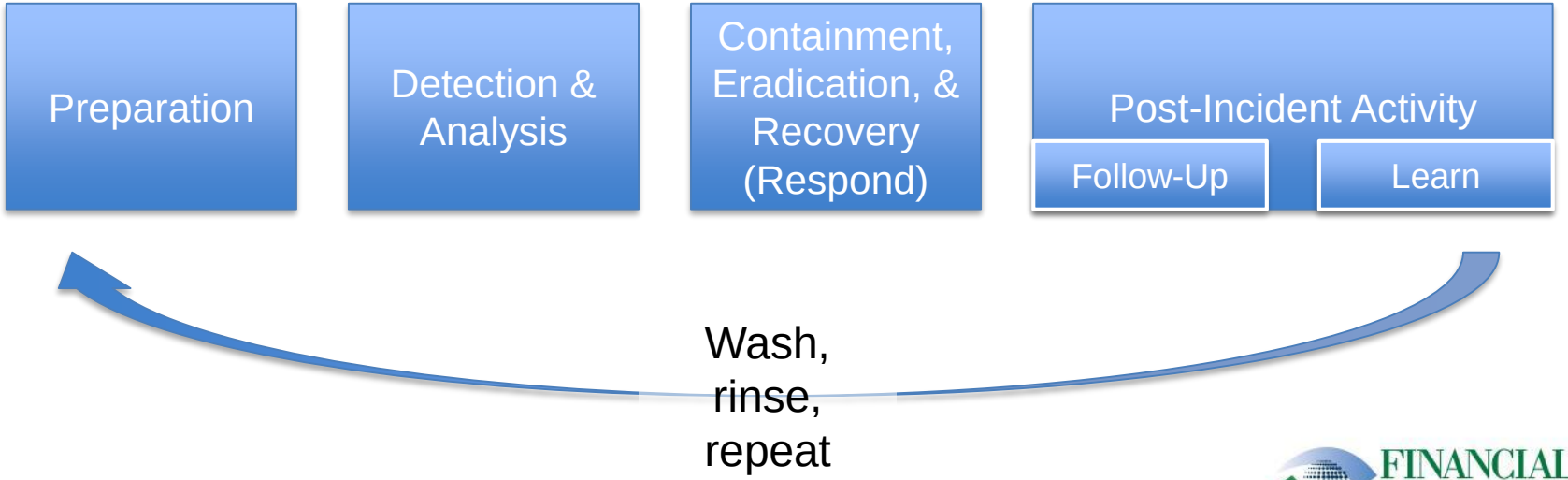
…so much better with friends

- What processes / practices do you follow?
- Collaborative staff training & exchange
- Preparing collective tools

- What is this thing?
- We are seeing a thing, this is what we think it is

- What are you doing about this?
- This is what we are doing about this
- Who did this?

- How can we improve our response speed?
- Whom should we have spoken to?
- How can we get these guys / stop this happening again?



So Why Share?

More Better Information, Faster

My first incident response team

- More effective use of limited resources
- New ideas
- Error checking
- Tying into existing initiatives / countermeasures
- Learning from others and vice versa
- Operational support when needed

A Few Thoughts on Preparation

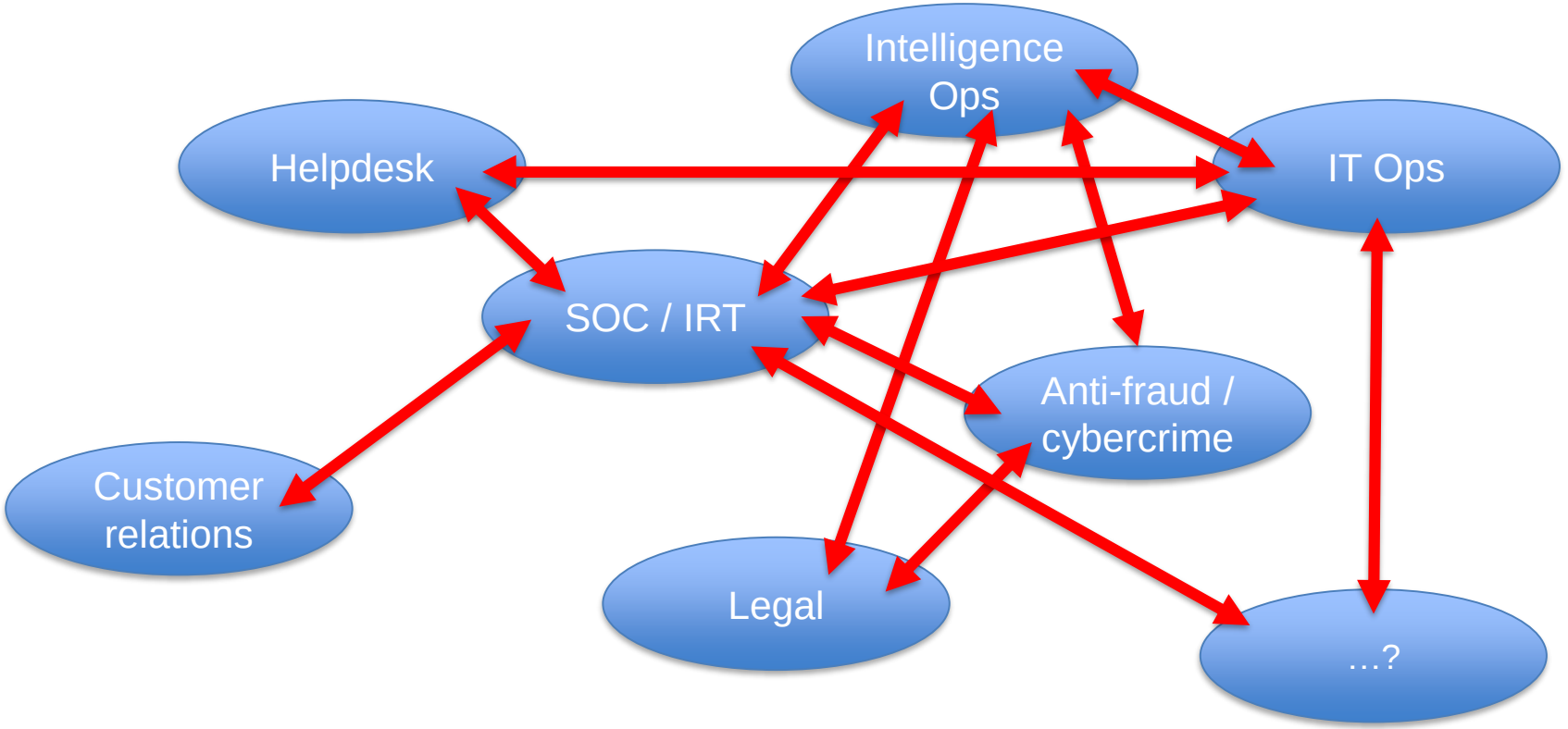
Improve Readiness Through Collaboration

- **War gaming** / simulations / collective red teaming
- Developing **trust networks**
- Common **policy framework** development
- Collective approach to **external stakeholders** (law enforcement, CERT, etc.)
- Common **standards** adoption - e.g. STIX/TAXII
- Common **platforms and channels** – portals, mailing lists, etc.
- Clearly defined **communications flows**
- After-action **reports and briefings**
- **Collective sell to senior management**

The intel team at work

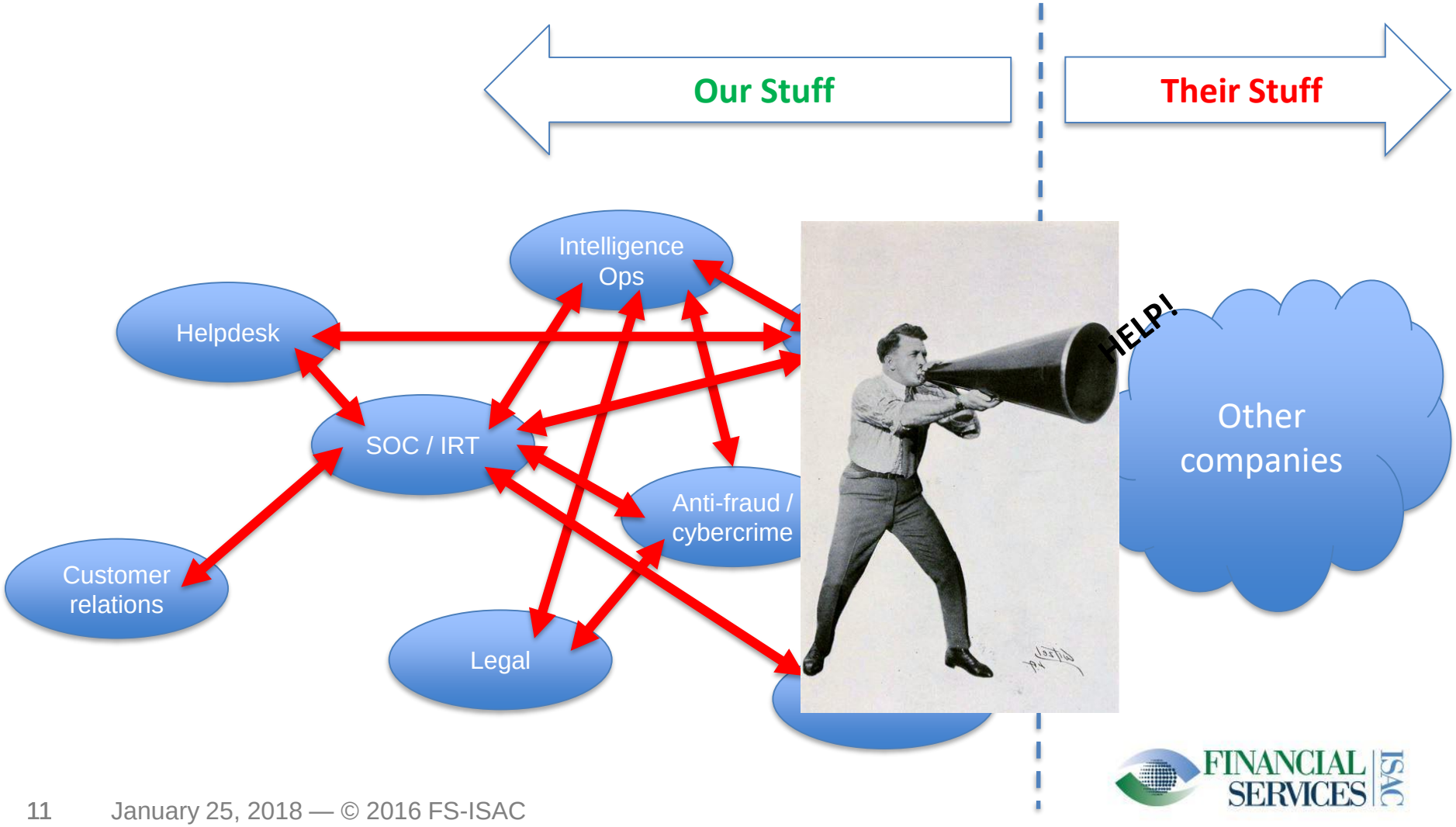
Where Does Everyone Fit?

Incident Response as a Capability, not just a Team



…Globally?

It's Not Just You



Collaboration Still is Difficult

Everybody Wants it, but…

Most cooperation takes place at preparation and post-incident levels.

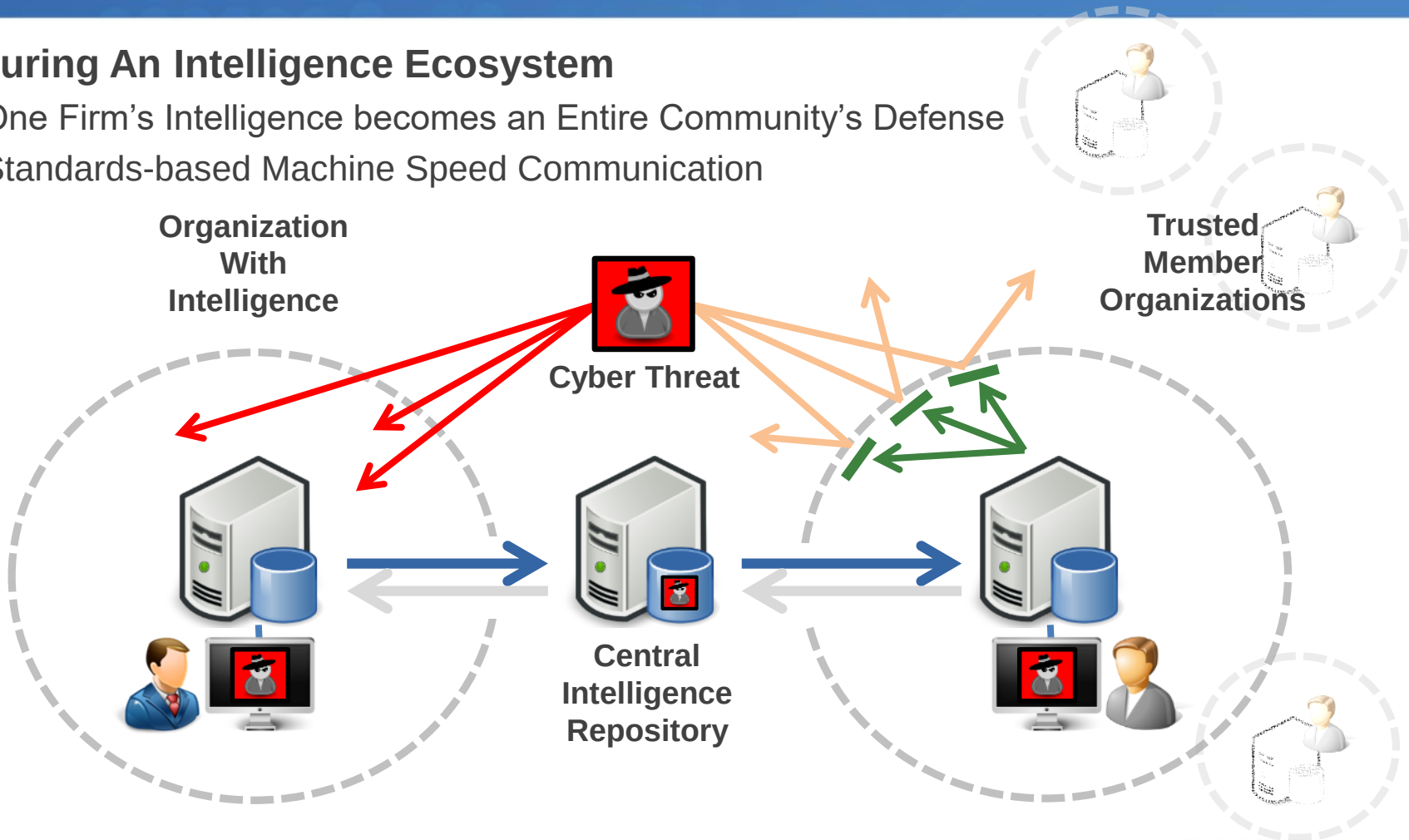
During-incident cooperation mainly via informal channels / small circles of trust.

That's just fine.

Automation and Intel / IR

Maturing An Intelligence Ecosystem

- One Firm's Intelligence becomes an Entire Community's Defense
- Standards-based Machine Speed Communication



 © 2016 FS-ISAC

Some Concerns?

Legal and Regulatory issues

- Can we be sued?
- Data protection rules
- Anti-competition rules

Trust Challenges

- Can we rely on counterparts?
- Is our data safe with them?
- Data quality
- Confidentiality

Effectiveness Issues

- How to ensure we don't step on each other's toes?

Business Issues

- How do we not look stupid while it's happening?

 © 2016 FS-ISAC

Thoughts on Improvement?

…?

 © 2016 FS-ISAC

Thank You!

John Salomon – Regional Director AUNZ (acting EMEA)
jsalomon@fsisac.com