

Threat Intelligence Sharing in the Financial Services Sector

Munich, Germany
February 24th, 2016



Ray Irving
Director CEMEA, FS-ISAC

rirving@fsisac.eu

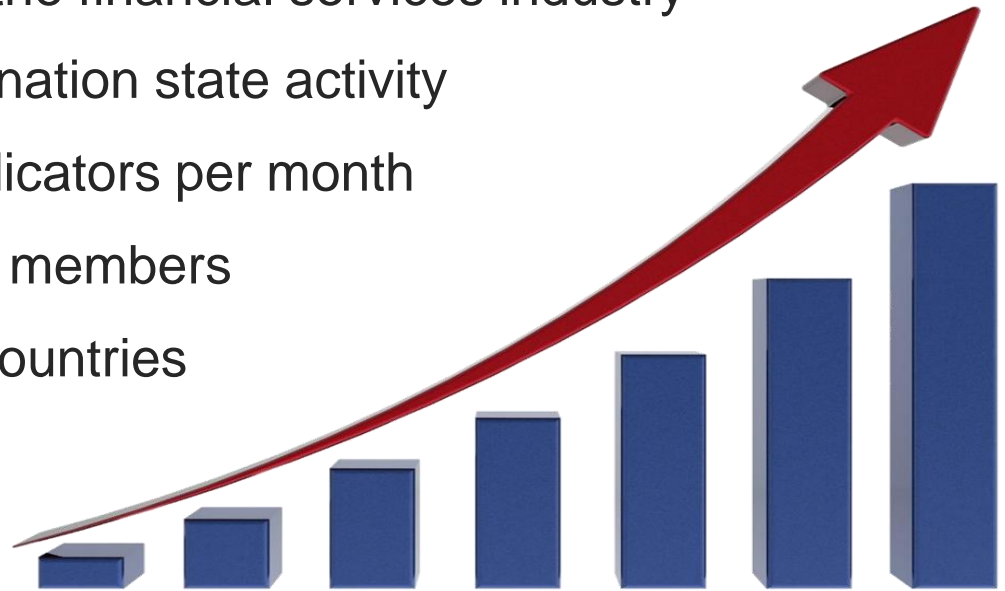
Agenda

- About FS-ISAC
- About Threat Intelligence
- How FS-ISAC works
- European Sharing Landscape
- FS-ISAC European Strategy 2016
- Next Steps

About FS-ISAC

MISSION: Share Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis

- A nonprofit private sector initiative formed in 1999
- Designed/supported/owned by the financial services industry
- Mitigate cybercrime, hacktivist, nation state activity
- Process thousands of threat indicators per month
- 2004: 68 members; 2015: 6700 members
- Share information globally, 38 countries



“The FS-ISAC is not a service provider, it’s a community...Like a neighborhood watch for cyber and physical hazards.” – A Longtime Member

Investment in Protecting the Sector

- Soltra Edge: first industry-owned Cyber Threat Intelligence Repository
 - Uses industry standard protocols: Structured Threat Information eXpression (STIX™) & Trusted Automated eXchange of Indicator Information (TAXII™)
- Civil litigation actions against botnet infrastructures. Last two targeted botnets targeting UK FIs and customers:
 - Shylock 2014
 - Ramnit 2015
- Sector Resilience Activities:
 - Cyber Attack Against Payments
 - All Hazards Playbook and US sector activities could scale to Europe
- Education and Training:
 - Annual Summits (2 in the US, 1 in Europe, 1 in APAC). “Who’s who” of risk & security executives participate and speak.
 - Member meetings, workshops and trainings.



The Case for Information Sharing

ONE ORGANIZATION'S INCIDENT BECOMES THE INDUSTRY RESPONSE



About Threat Intelligence

What is intelligence?

“[I]ntelligence is more than information. It is knowledge that has been specially prepared for a customer’s unique circumstances.

... The word ‘**knowledge**’ highlights the need for human involvement. Intelligence collection systems produce.... data, not intelligence; only the human mind can provide that special touch that makes sense of data for different customers’ requirements.

.... The special processing that partially defines **intelligence is the continual collection, verification, and analysis of information that allows us to understand the problem or situation in actionable terms** and then tailor a product in the context of the customer’s circumstances.

.... If any of these essential attributes is missing, then the product remains information rather than intelligence.”

– Captain William Brei, ‘Getting Intelligence Right,’
US JMIC Publication



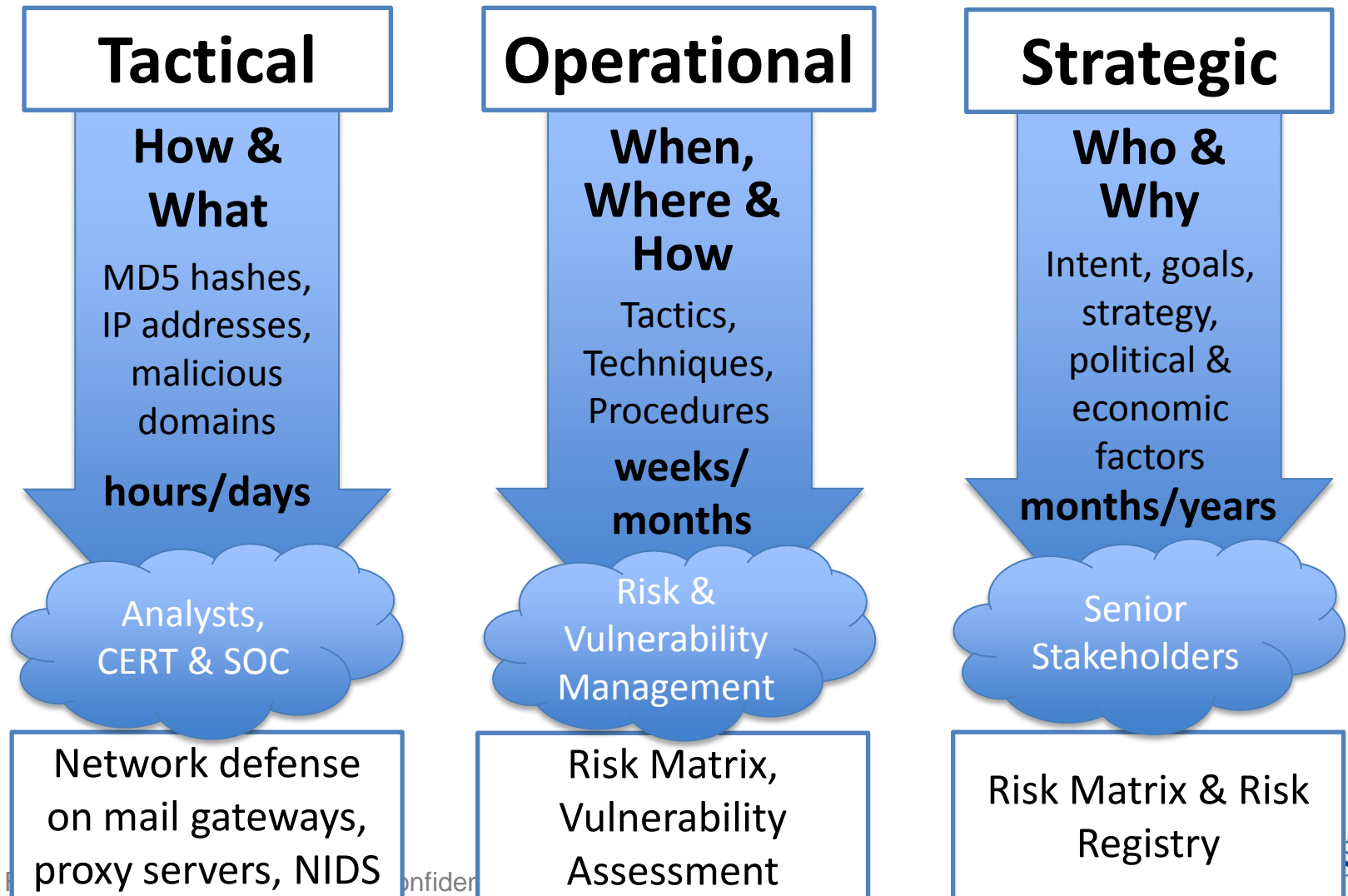
Cyber Intelligence Consumers

Senior Leaders: support **business strategy** by delivering insight into **cyber threats** which could (or have) impacted **risk thresholds**.

Middle Managers: **timely, relevant & applied** within a **risk management framework** to allow for **review & testing of policy & controls**.

Network Defenders tactical feeds of **technical indicators** supports the **real-time defence of networks** and provides a **measure of the effectiveness of IT security controls**.

Types of Threat Intelligence

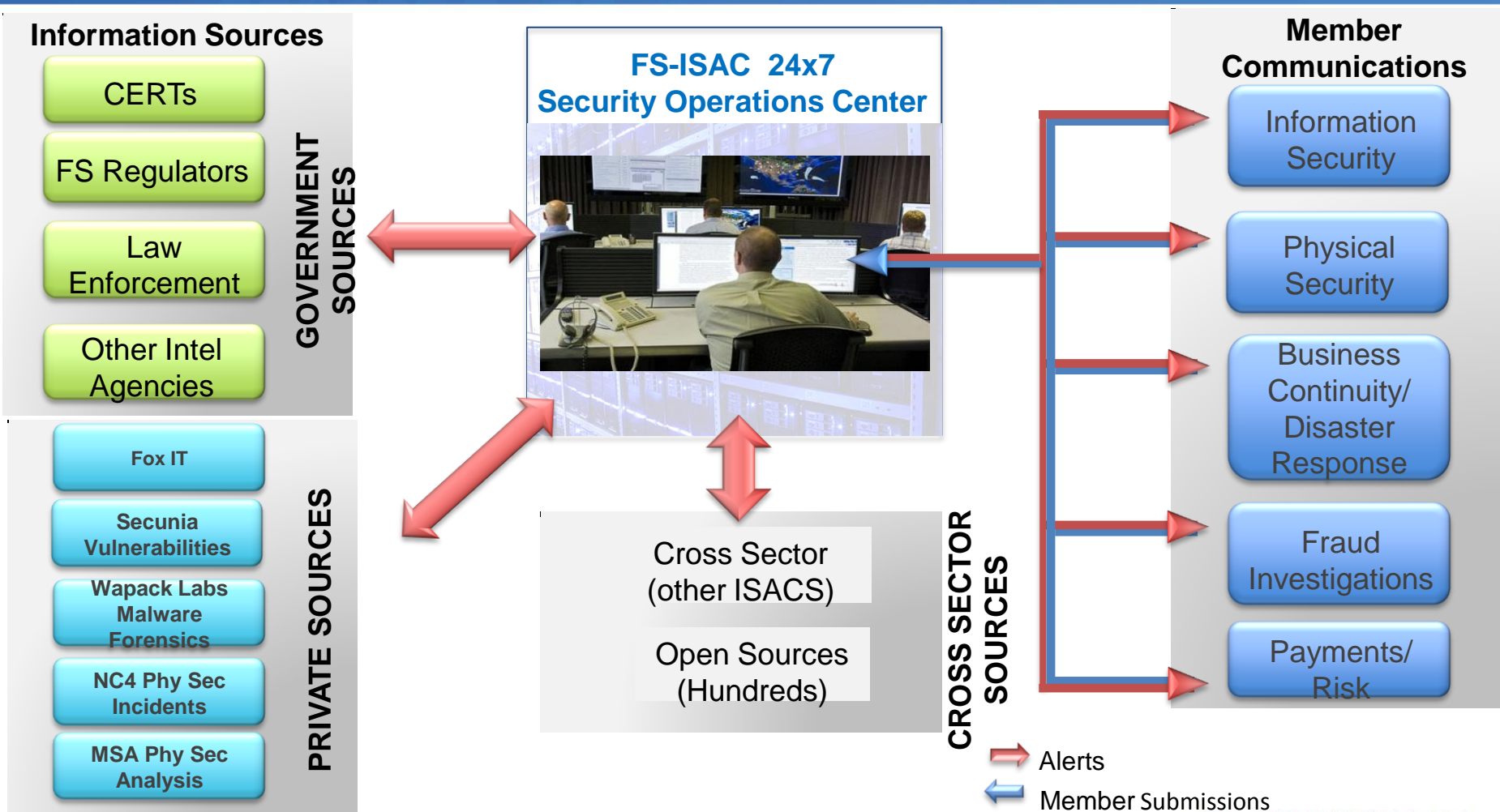


How FS-ISAC Works

Tools for sharing

Tool	Intelligence Shared	Target Audience	Type of Intel
Cyber Intelligence mailing list	~40 mails/day: near real time observations, incidents, requests and queries from the community.	Threat Intelligence, Security Operations & Malware Analysts	Tactical, Operational
Portal Alerts	~20 alerts/day: Cyber and Physical Threats & Incidents; Vulnerabilities; Collective Intelligence.	Threat Intell. & Malware Analysts, SOC and Physical security staff.	Tactical, Operational
Daily Summary	Daily overview of all alerts.	Head of Intelligence or Security Operations.	Tactical, Operational
Bi-weekly Threat Calls	Threat landscape review including 3 rd party briefings and threat level discussion.	Risk and Information Security Management	Operational, Strategic
Member Meetings & Summits	Member presentations on experiences and best practices.	All information security staff.	Operational, Strategic

FS-ISAC Information Flow



Traffic Light Protocol



Red: Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group



Amber: This information may be shared with FS-ISAC members.



Green: Information may be shared with FS-ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums

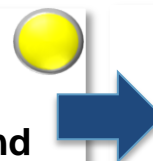


White: This information may be shared freely and is subject to standard copyright rules

Member Reports
Incident to Cyber
Intel list, or via
anonymous submission



Members or IAT
respond in real time
with initial analysis and
recommendations



IAT completes analysis,
anonymizes the source, and
generates alert to general
membership



Types of FS-ISAC Alerts



Alert Types



Criticality and Priority:

- ANC = Priority – 1-10, 8-10 is high priority
- CYV = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- CYT = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- COI – No Criticality Metric
- PHT = Risk – 1-10. 8-9 is Urgent, 10 is Crisis



Observables



Indicators



Incidents



TTPs

European Sharing Landscape

UK Finance Sector Cyber Related Collaboration Groups

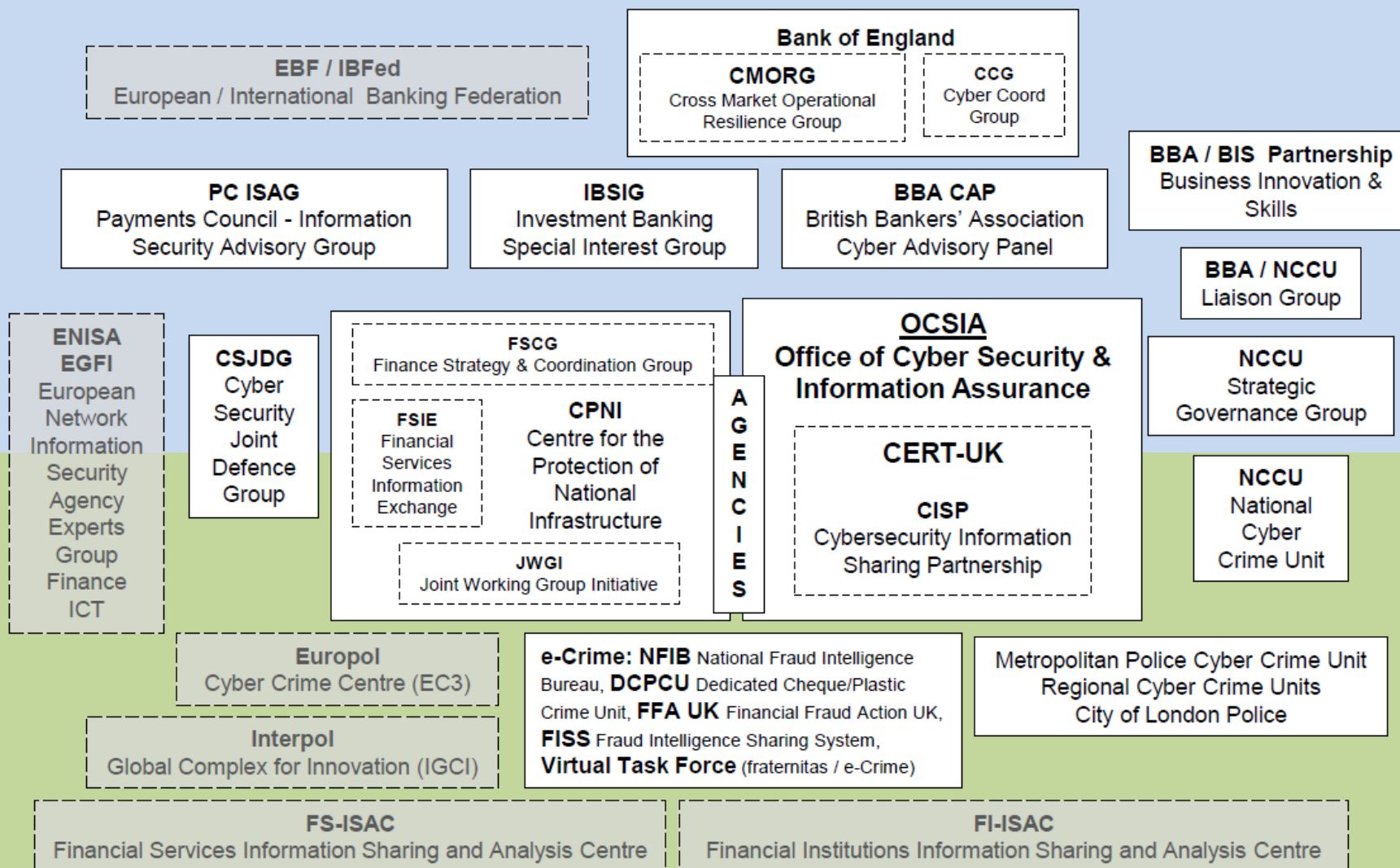
and their National and International Links

STRATEGY / POLICY

STRATEGY / POLICY

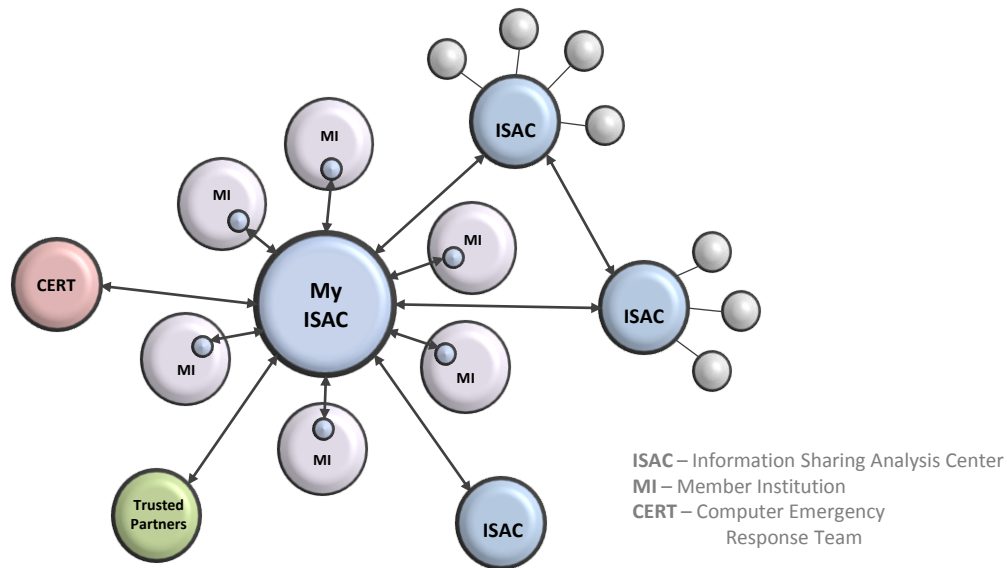
COLLABORATION /
INTELLIGENCE SHARING

COLLABORATION /
INTELLIGENCE SHARING

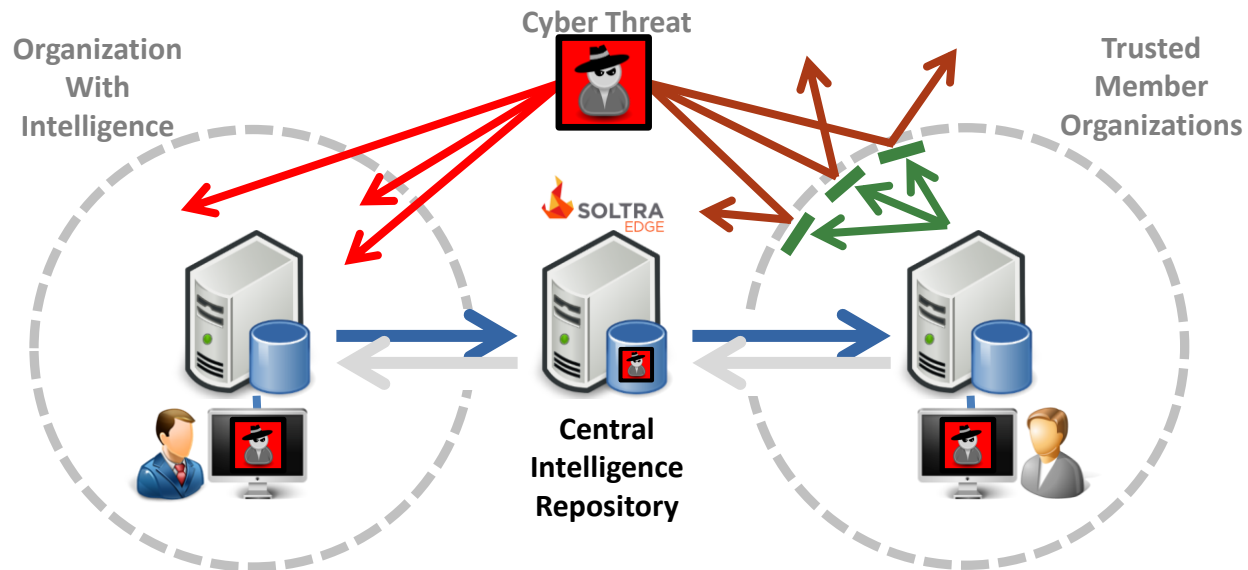


Community Defense Vision

- Intelligence Ecosystem
 - One Firm's Intelligence becomes an Entire Community's Defense



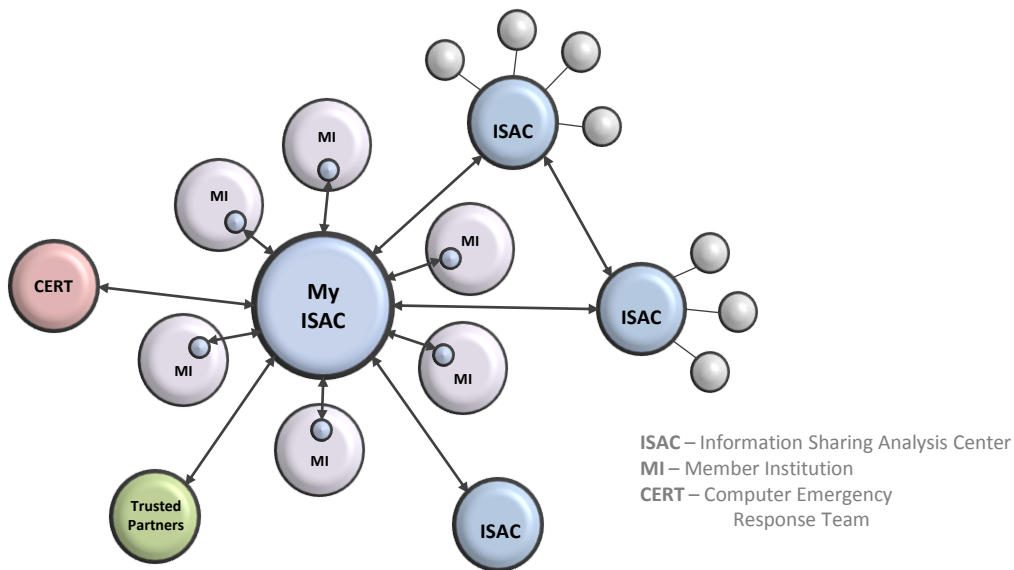
Automated Community Defense



FS-ISAC European Strategy 2016

“Build Trusted Communities”

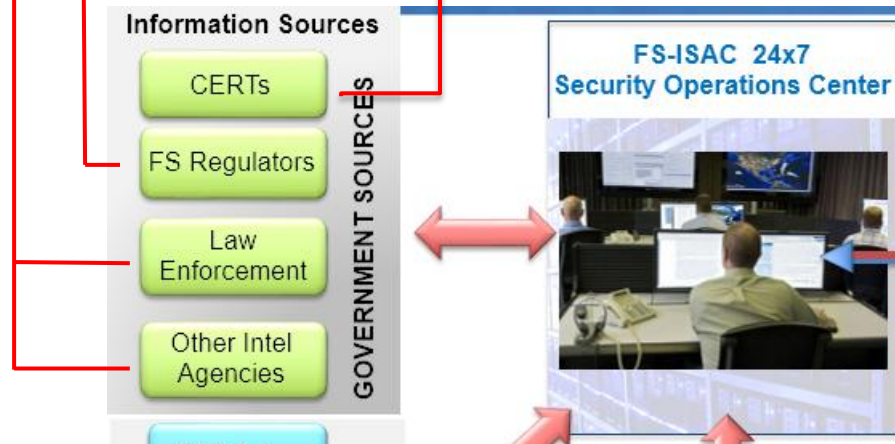
	Task	What / How?
1.	Build Trusted Communities	<ol style="list-style-type: none">Link into in-country sharing schemesEncourage / develop the JWGIFS-ISAC (add value by linking national into regional /global network)



- i. & iii. - Most EU countries have some degree of in-country sharing:
- FS-ISAC can be the proxy for sharing between in country and regional sharing schemes.
 - Country-based memberships can encourage anonymous sharing.
 - FS-ISAC LE/Govt relationships can help mitigate internal PPP issues.

“Engagement & Collaboration”

	Task	What / How?
2.	Engagement / Collaboration: <ul style="list-style-type: none"> a. Law Enforcement b. Government c. Regulators 	Link into / influence key nodes: Operational: <ul style="list-style-type: none"> i. Europol (EC3) ii. In-country LE / CERTs Policy / Regulation: <ul style="list-style-type: none"> i. European Banking Federation (EBF) ii. European Commission / Parliament iii. ENISA iv. National Banking Associations



Next Steps

- If you are an FS entity:
 - Cost to join FS-ISAC based on asset value (banks) or revenue (insurance).
 - We are a non profit so membership fees are very reasonable.
 - Talk to us about joining for a 6 month evaluation period.
- If you are a CERT:
 - We would like to establish a formal relationship with you.
 - As per the CERT UK model: this could be a Memorandum of Understanding allowing sharing of green and clear intel/products plus “as needed” sharing of amber intelligence.
 - Open to other suggestions.

Contact Information

Ray Irving

Director,
Continental Europe, Middle East
and Africa

rirving@fsisac.eu

www.fsisac.com