RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

The Role of the ISACs in Critical Infrastructure Resilience

SESSION ID: CLE-T10

Denise Anderson
Chair-National Council of ISACs

#RSAC

Agenda

- What is an ISAC?
- Examples of ISACs, their activities and reach,
- Overview of FS-ISAC as a successful model for information sharing,
- What is the National Council of ISACs?
- Overview of Council Activities,
- Public-Private Partnerships,
- Specific Case Studies,
- The Future of Information Sharing

What is an ISAC?

Why ISACs?

Why ISACs?

- Trusted entities established by CI/KR owners and operators.
- Comprehensive sector analysis aggregation/ anonymization
- Reach-within their sectors, with other sectors, and with government to share critical information.
- All-hazards approach
- Threat level determination for sector
- Operational-timely accurate actionable

ISACs

- Communications ISAC
- Defense Industrial Base ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Information Technology ISAC
- Maritime ISAC
- Multi-State ISAC

ISACs

- National Health ISAC
- Oil and Natural Gas ISAC (ONG)
- Over the Road & Motor Coach ISAC
- Public Transit ISAC
- Real Estate ISAC
- Research and Education ISAC
- Supply Chain ISAC
- Surface Transportation ISAC
- Water ISAC

Other Operational Sectors and Upcoming ISACs

- **Automotive**
- **Aviation**
- Food & Ag
- Nuclear
- Chemical
- Critical Manufacturing

Examples of ISACs

Activities and Reach

Communications ISAC

- The DHS National Coordinating Center partners with the private sector in the ISAC and provides 24x7 operational support
- Members include communications equipment and software vendors, wire line communications providers, wireless communications providers, including satellite providers, Internet Service Provider backbone networks
- www.ncs.gov/ncc

Defense Industrial Base ISAC

- The DIB ISAC's coverage includes contractors to the Department of Defense
- All approach to securing the DIB Supply Chain hazards
- Regional outreach to reach tier two and three companies
- www.dibisac.net

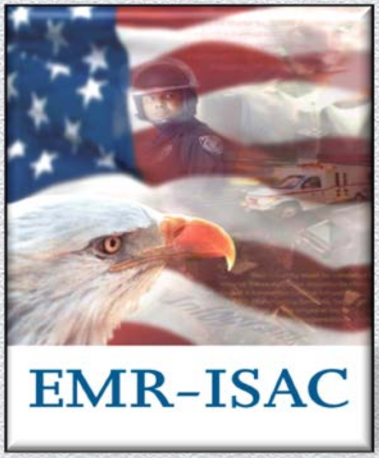
DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
SECTOR COORDINATING COUNCIL

Electricity Sector ISAC

- The ES-ISAC's coverage includes bulk power system entities and 18 Reliability Coordinators and covers the entire continental United States and Canada
- Working on developing the necessary communication and participation with non-bulk power system entities and their critical suppliers
- www.esisac.com

Emergency Management Response ISAC

- The EMR-ISAC initiated in 2000 by a FEMA contract, operates from the National Emergency Training Center in Emmitsburg, MD
- Reaches over 40,000 ESS departments and agencies directly, thousands more reached through ESS associations, departments and agencies as well as state and local fusion centers
- www.usfa.dhs.gov/emr-isac



Financial Services ISAC

- The FS-ISAC is the only industry forum for collaboration on critical security threats facing the financial services sector
- Over 5,000 direct members and 30 member associations
- Ability to reach 99% of the banks and credit unions and 85% of the securities industry, and over 50% of the insurance industry
- www.fsisac.com

Information Technology ISAC

- The IT-ISAC reaches 90% of all desktop operating systems, 85% of all databases; 76% of the global microprocessor market; 85% of all routers and 65% of software security
- www.it-isac.org

Maritime Security ISAC

- Established in 1988
- Non-profit, member driven organization representing ocean carriers, cruise lines, port facilities and terminals, logistics providers, importers, exporters and related maritime industries throughout the world
- http://www.maritimesecurity.org/

Multi-State ISAC

- The MS-ISAC includes all 50 States, the District of Columbia, five U.S. Territories, one local governments per state and all state homeland security offices
- The MS-ISAC continues to broaden its local government participation to include all of the approximate 39,000 municipalities and fusion centers
- www.msisac.org

National Health ISAC

- The NH-ISAC serves to protect the nation's healthcare and public health critical infrastructure against security threats and vulnerabilities.
- Founded in 2010 leveraging Center for Technology Innovation at Kennedy Space Center
- Healthcare and Public Health organizations
- www.nhisac.org

Oil and Natural Gas ISAC

- The ONG-ISAC serves to protect the nation's exploration and production, transportation, refining, and delivery systems from cyber-attacks
- Founded in 2014 is the central reservoir of cyber threat information for the oil and natural gas industry
- http://ongisac.org/

ONG-ISAC

Public Transit ISAC

- The PT-ISAC was created by The American Public Transportation Association (APTA). APTA is designated by the US Department of Transportation as the sector coordinator for the US public transit industry
- Members serve more than 90% of persons using public transportation in the United States and Canada
- www.surfacetransportationisac.org/APTA.asp

Real Estate ISAC

- The RE-ISAC was created by the Real Estate Roundtable in 2003
- Membership comprised of 11 major associations such as BOMA, IREM, American Hotel & Lodging, National Apartment Association, International Institute of Shopping Centers, Real Estate Roundtable
- http://reisac.org/

Real Estate ISAC Information Sharing and Analysis Center

Research and Education ISAC

- Supported by Indiana University and through relationships with EDUCAUSE and Internet2, the REN-ISAC is an integral part of higher education's strategy to improve network security specifically designed to support the unique environment and needs of over 1,400 organizations connected to served higher education and research networks
- Ability to reach 4,000 EDU organizations
- www.ren-isac.net

Supply Chain ISAC

- The SC ISAC includes over 661 manufacturers & shippers, cargo carriers (air, rail, highway and maritime), consignees, supply chain service suppliers, law enforcement and federal government agencies, reaching about 1,700 users
- Launched in June 2006 with the announcement of its sponsorship by the International Cargo Security Council (ICSC) at the ICSC Annual Conference
- www.secure.sc-investigate.net/SC-ISAC

Surface Transportation ISAC

- Created by the Association of American Railroads in 2002 at the request of the Secretary of Transportation
- The ST-ISAC supports 95% of the North American freight railroad infrastructure
- www.surfacetransportationisac.org

Water-ISAC

- Currently provides security information to water and wastewater utilities that provide services to more than 65% of the American population

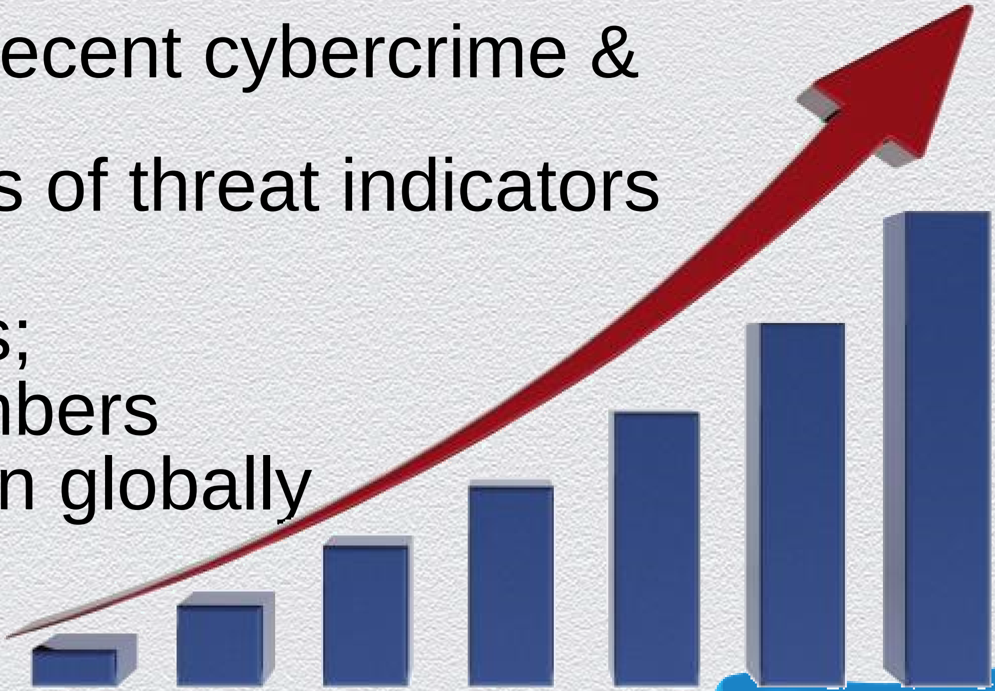
- www.waterisac.org

Overview of FS-ISAC

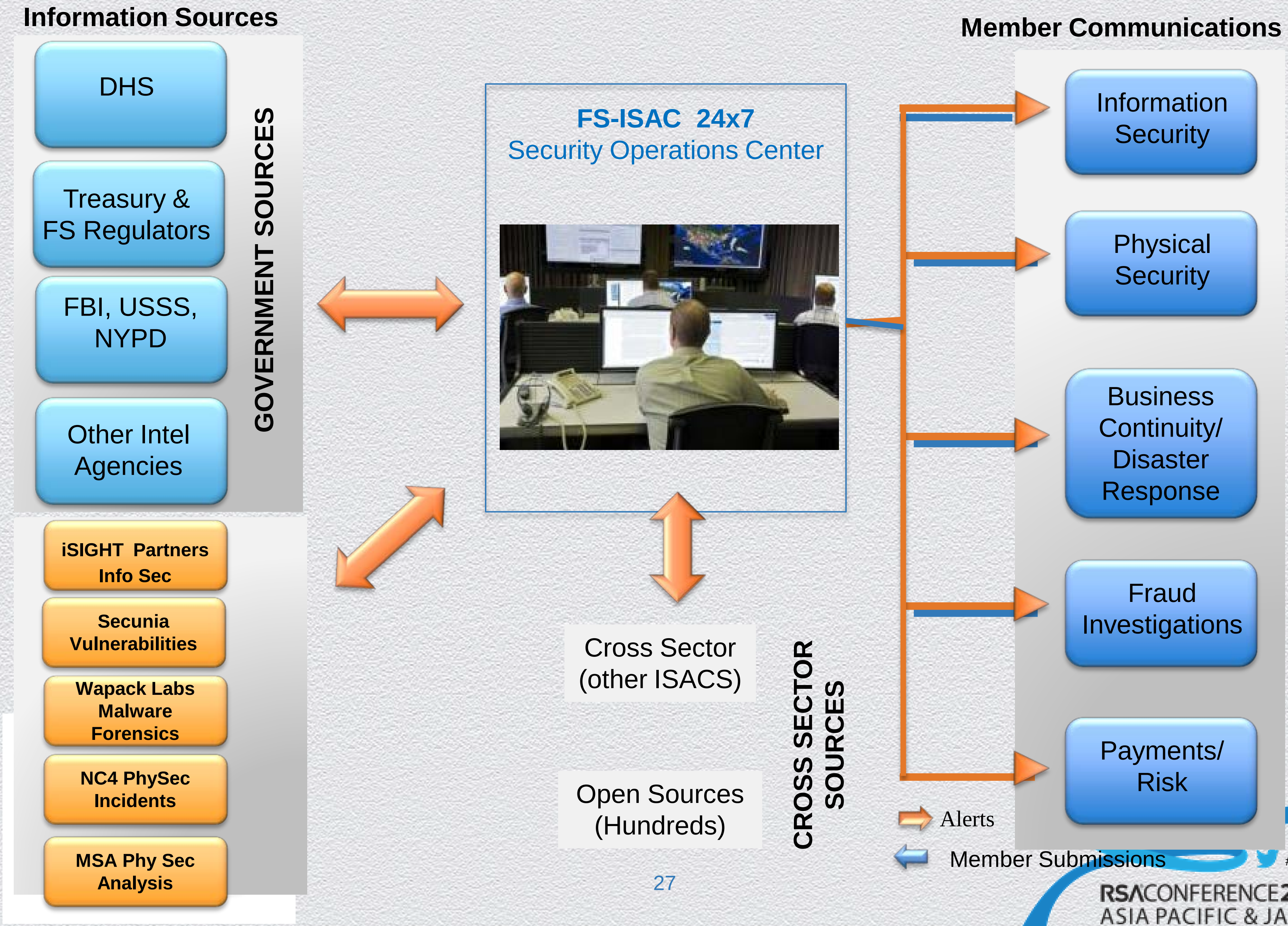
Example of a Successful Model for Sharing

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

- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Assist to mitigate recent cybercrime & fraud activity
- Process thousands of threat indicators per month
- 2004: 68 members;
- 2014: 5,000+ members
- Sharing information globally



FS-ISAC Operations



Information Sources

DHS

Treasury & FS Regulators

FBI, USSS, NYPD

Other Intel Agencies

GOVERNMENT SOURCES

iSIGHT Partners Info Sec

Secunia Vulnerabilities

Wapack Labs Malware Forensics

NC4 PhySec Incidents

MSA Phy Sec Analysis

FS-ISAC 24x7
Security Operations Center

Cross Sector (other ISACS)

Open Sources (Hundreds)

CROSS SECTOR SOURCES

Member Communications

Information Security

Physical Security

Business Continuity/ Disaster Response

Fraud Investigations

Payments/ Risk

Alerts

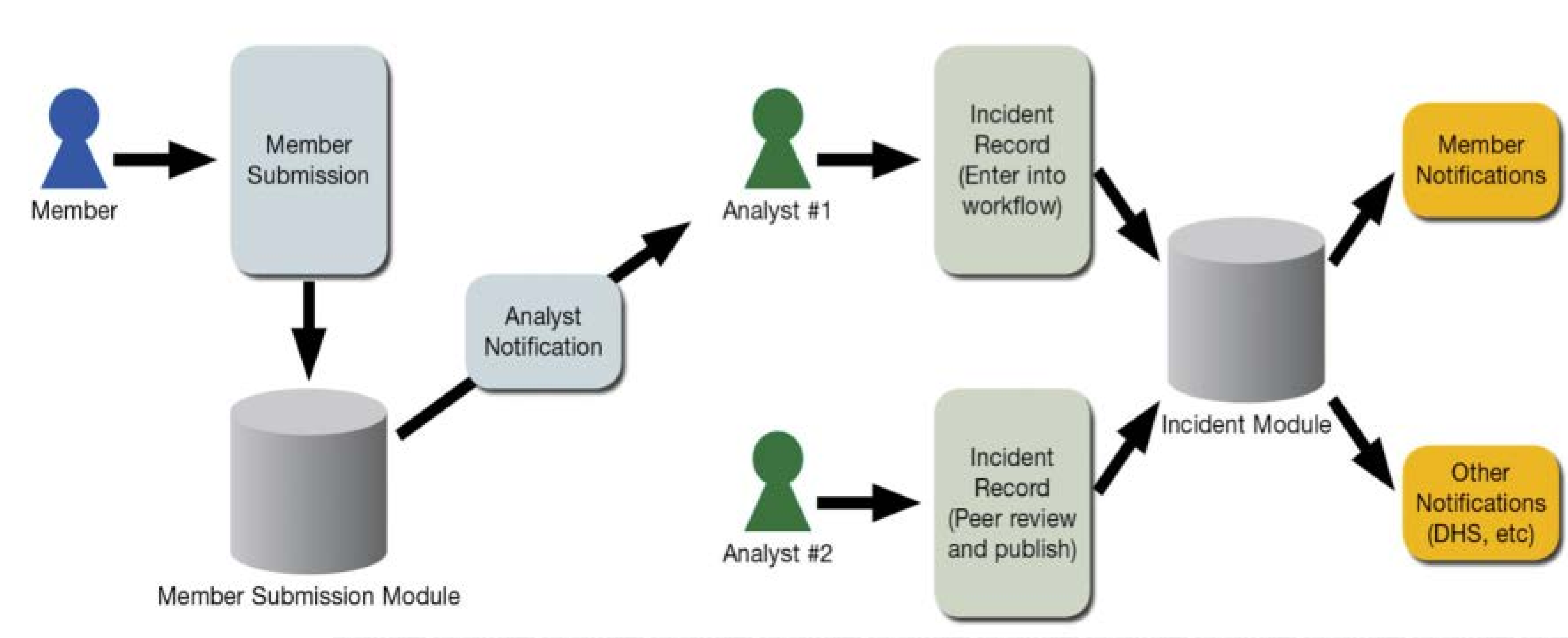
Member Submissions

Traffic Light Protocol (TLP)

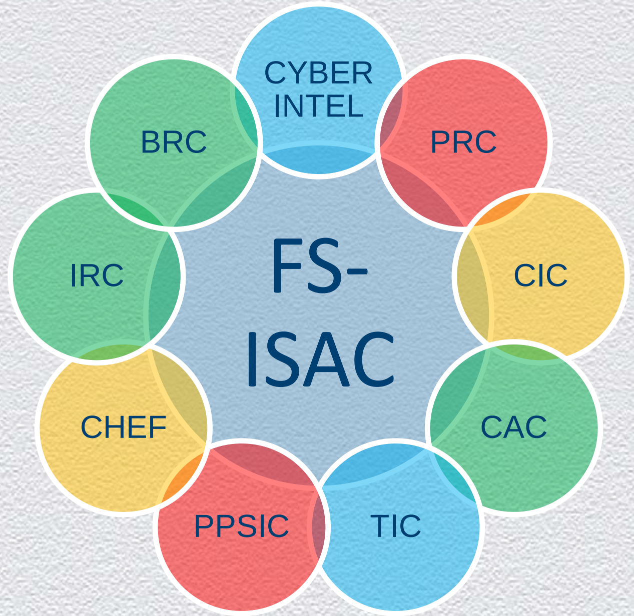
- Restricted to a defined group (e.g., only those present in a meeting.) Information labeled **RED** should not be shared with anyone outside of the group
- **AMBER** information may be shared with FS-ISAC members.
- **GREEN** Information may be shared with FS-ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums
- **WHITE** information may be shared freely and is subject to standard copyright rules

Member Submissions Via the Secure Portal

- **Anonymous or Attributed**
  Submission Types: Cyber Incident, Physical Incident or Document Upload



How FS-ISAC Works: Circles of Trust



- Clearing House and Exchange Forum (CHEF)
- Payments Risk Council (PRC)
- Payments Processor Information Sharing Council (PPISC)
- Business Resilience Committee (BRC)
- Threat Intelligence Committee (TIC)
- Community Institution Council (CIC)
- Insurance Risk Council (IRC)
- Compliance and Audit Council (CAC)
- Cyber Intelligence Listserv
- Education Committee
- Product and Services Review Committee
- Survey Review Committee
- Security Automation Working Group (SAWG)

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

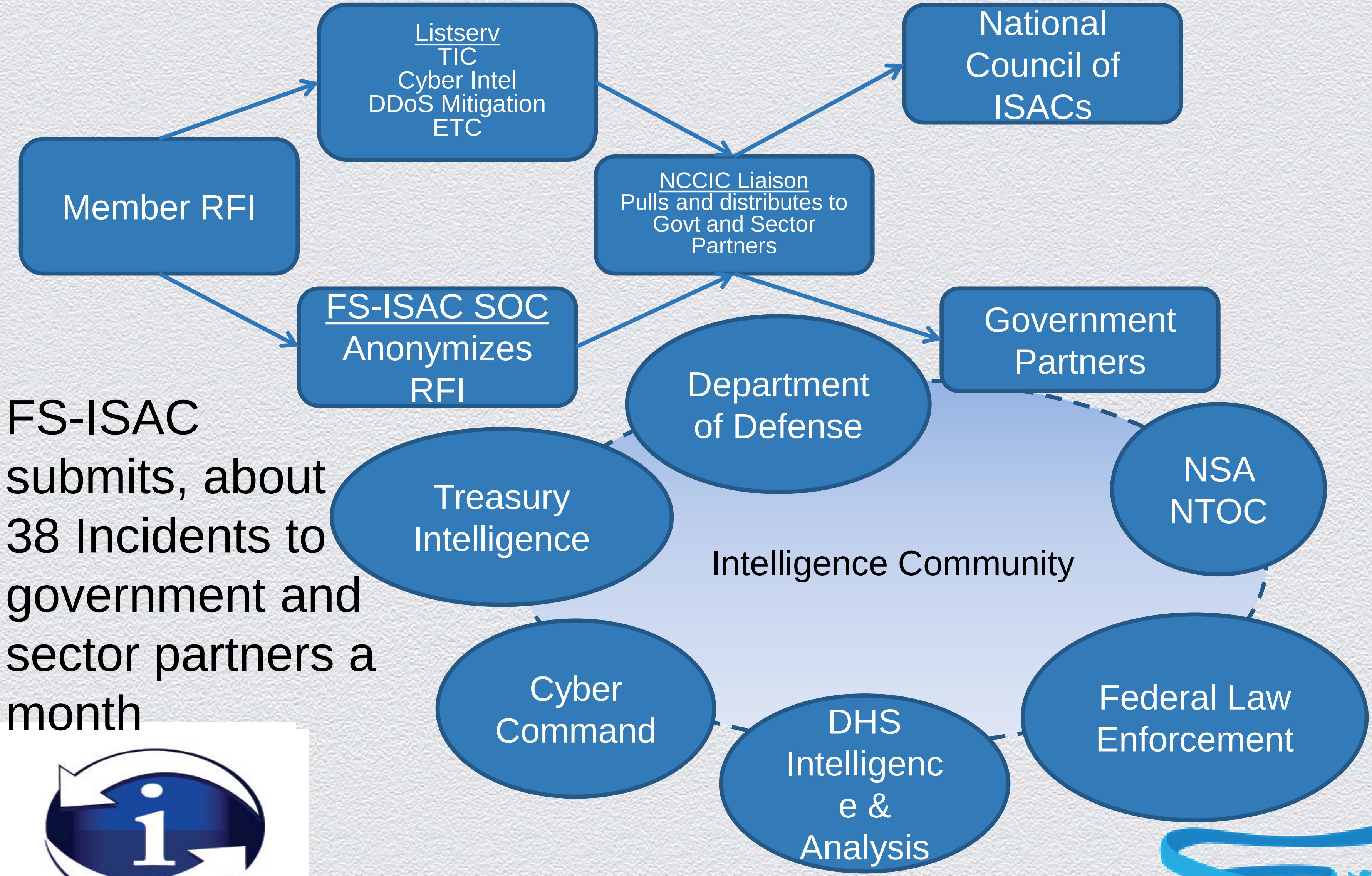
→

Members respond in real time with initial analysis and recommendations

→

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

Information Sharing Flow - External



Member RFI

Listserv
TIC
Cyber Intel
DDoS Mitigation
ETC

FS-ISAC SOC
Anonymizes RFI

NCCIC Liaison
Pulls and distributes to Govt and Sector Partners

National Council of ISACs

Government Partners

Intelligence Community

Department of Defense

Treasury Intelligence

NSA NTOC

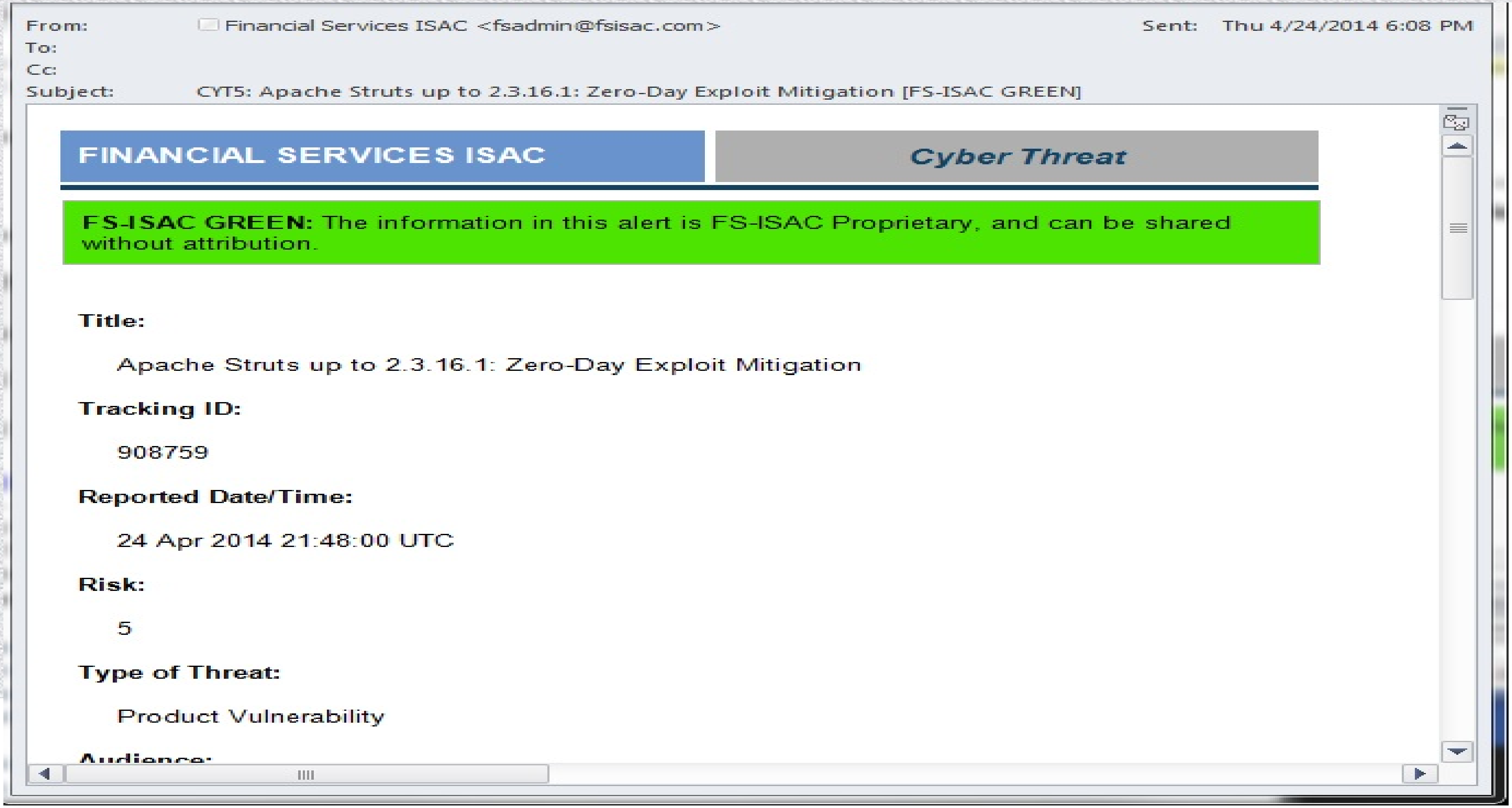
Cyber Command

DHS Intelligence & Analysis

Federal Law Enforcement

FS-ISAC submits, about 38 Incidents to government and sector partners a month

Sample Alert



From: ☐ Financial Services ISAC <fsadmin@fsisac.com> Sent: Thu 4/24/2014 6:08 PM
To:
Cc:
Subject: CYT5: Apache Struts up to 2.3.16.1: Zero-Day Exploit Mitigation [FS-ISAC GREEN]

FINANCIAL SERVICES ISAC | *Cyber Threat*

FS-ISAC GREEN: The information in this alert is FS-ISAC Proprietary, and can be shared without attribution.

Title:

Apache Struts up to 2.3.16.1: Zero-Day Exploit Mitigation

Tracking ID:

908759

Reported Date/Time:

24 Apr 2014 21:48:00 UTC

Risk:

5

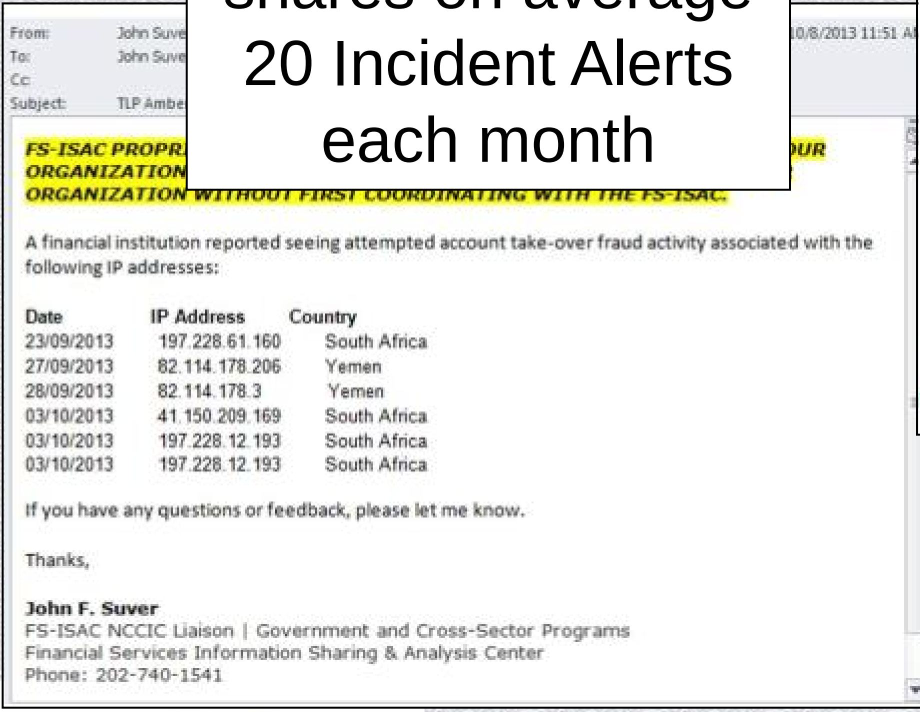
Type of Threat:

Product Vulnerability

Audience:

FS-ISAC Products

FS-ISAC Incident Alert: FS-ISAC shares on average 20 Incident Alerts each month



From: John Suve

To: John Suve

Cc:

Subject: TLP Ambe

10/8/2013 11:51 A

FS-ISAC PROPR … **OUR ORGANIZATION** … **ORGANIZATION WITHOUT FIRST COORDINATING WITH THE FS-ISAC.**

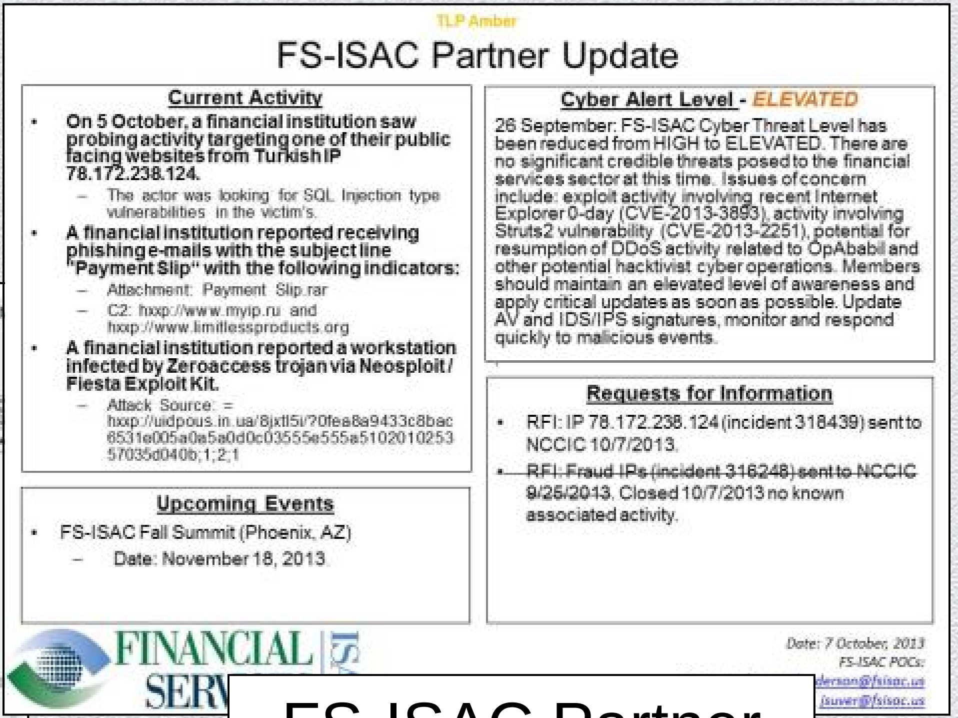
A financial institution reported seeing attempted account take-over fraud activity associated with the following IP addresses:

Date	IP Address	Country
23/09/2013	197.228.61.160	South Africa
27/09/2013	82.114.178.206	Yemen
28/09/2013	82.114.178.3	Yemen
03/10/2013	41.150.209.169	South Africa
03/10/2013	197.228.12.193	South Africa
03/10/2013	197.228.12.193	South Africa

If you have any questions or feedback, please let me know.

Thanks,

John F. Suver
FS-ISAC NCCIC Liaison | Government and Cross-Sector Programs
Financial Services Information Sharing & Analysis Center
Phone: 202-740-1541



TLP Amber

FS-ISAC Partner Update

Current Activity

- **On 5 October, a financial institution saw probing activity targeting one of their public facing websites from Turkish IP 78.172.238.124.**
  - The actor was looking for SQL Injection type vulnerabilities in the victim's.
- **A financial institution reported receiving phishing e-mails with the subject line "Payment Slip" with the following indicators:**
  - Attachment: Payment Slip.rar
  - C2: hxxp://www.myip.ru and hxxp://www.limitlessproducts.org
- **A financial institution reported a workstation infected by Zeroaccess trojan via Neosploit / Fiesta Exploit Kit.**
  - Attack Source: = hxxp://uidpous.in.ua/8jxtl5i/?0fea8a9433c8bac6531e005a0a5a0d0c03555e555a510201025357035d040b;1;2;1

Upcoming Events

- FS-ISAC Fall Summit (Phoenix, AZ)
  - Date: November 18, 2013

Cyber Alert Level - *ELEVATED*

26 September: FS-ISAC Cyber Threat Level has been reduced from HIGH to ELEVATED. There are no significant credible threats posed to the financial services sector at this time. Issues of concern include: exploit activity involving recent Internet Explorer 0-day (CVE-2013-3893), activity involving Struts2 vulnerability (CVE-2013-2251), potential for resumption of DDoS activity related to OpAbabil and other potential hacktivist cyber operations. Members should maintain an elevated level of awareness and apply critical updates as soon as possible. Update AV and IDS/IPS signatures, monitor and respond quickly to malicious events.

Requests for Information

- RFI: IP 78.172.238.124 (incident 318439) sent to NCCIC 10/7/2013.
- ~~RFI: Fraud IPs (incident 316248) sent to NCCIC 9/26/2013~~. Closed 10/7/2013 no known associated activity.

Date: 7 October, 2013
FS-ISAC POCs:
derson@fsisac.us
jsuver@fsisac.us

FS-ISAC Partner Update: FS-ISAC shares on average 21 Partner Update Slides each month

#RSAC

What is the National Council of ISACs?

Overview of Activities

National Council of ISACs

- Began meeting in 2003 to address common concerns and cross-sector interdependencies

- Volunteer group of ISACs who meet monthly to develop trusted working relationships among sectors on issues of common interest and work on initiatives of value to CI/KR

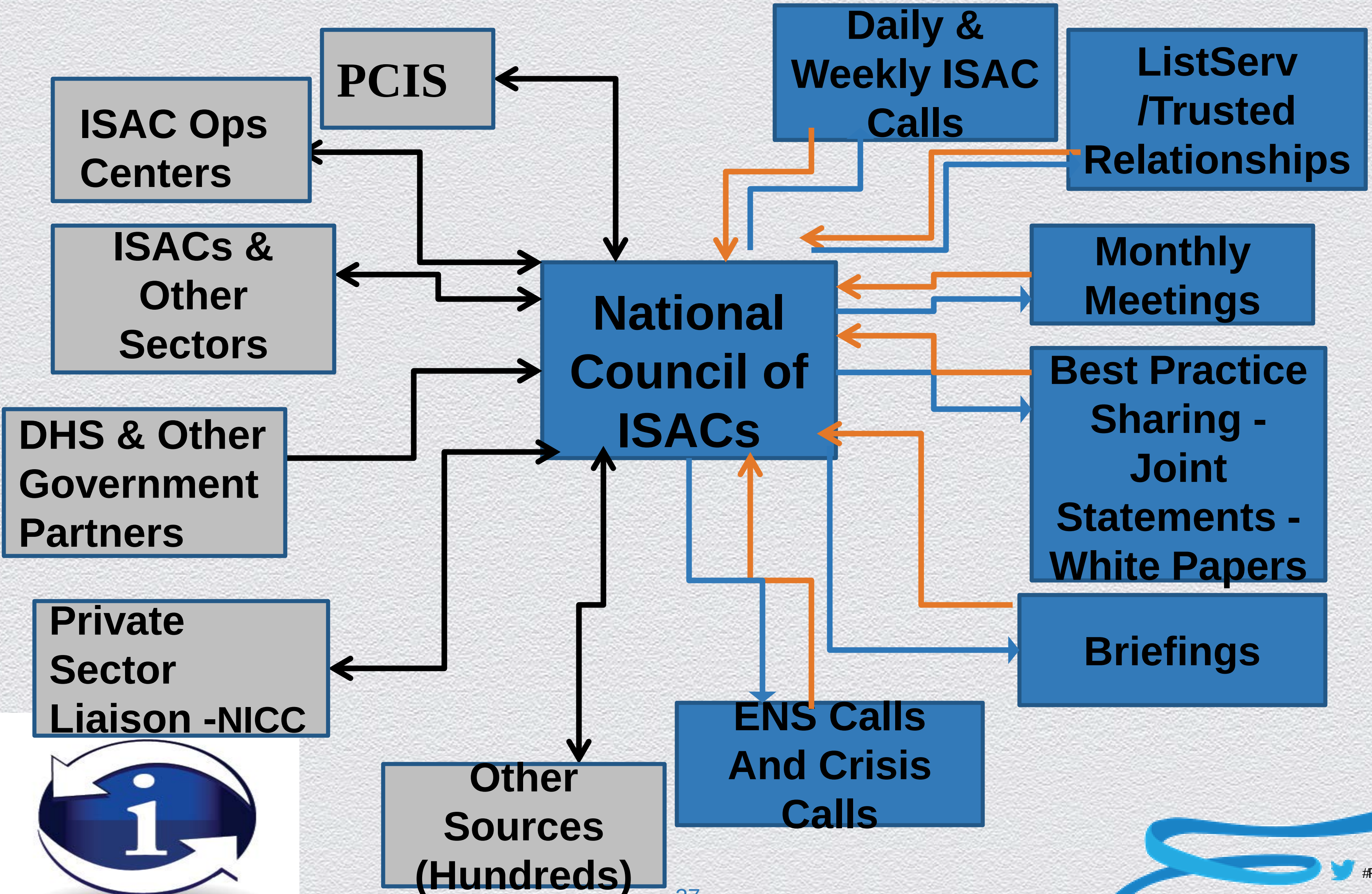
NCI Structure

- National Council of ISACs: four designated operational representatives from each ISAC sit on the Council.
- ISAC Plus: all other entities/representatives such as operations centers who participate in information sharing
- Leadership:

Chair: Denise Anderson-FS-ISAC

Vice-Chair: Scott Algeier-IT-ISAC

Secretary: Josh Poster-ST-ISAC



Information Sources

Communications

PCIS

ISAC Ops Centers

ISACs & Other Sectors

DHS & Other Government Partners

Private Sector Liaison -NICC

Other Sources (Hundreds)

National Council of ISACs

Daily & Weekly ISAC Calls

ListServ /Trusted Relationships

Monthly Meetings

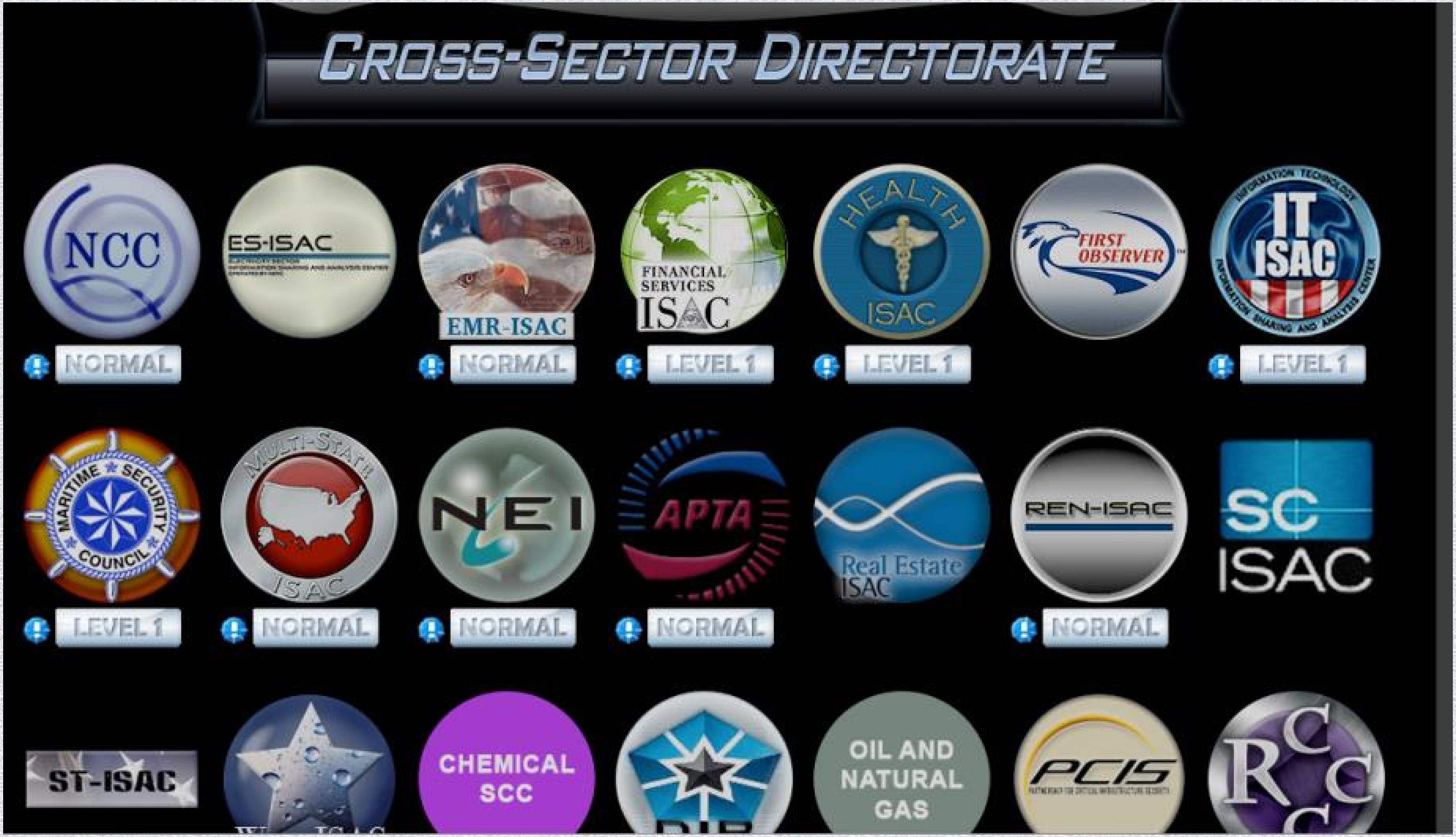
Best Practice Sharing - Joint Statements - White Papers

Briefings

ENS Calls And Crisis Calls

Examples of Activities

- Increase involvement of sectors without ISACs
- **Cross Sector Information Sharing Portal**
- **Private Sector Liaison with the NICC**
- Drills/Exercises Such as NLEs, Cyber Storm
- Implement Real-Time sector Threat Level Reporting
  - Directorate


CROSS-SECTOR DIRECTORATE
NCC
NORMAL
ES-ISAC
EMR-ISAC
NORMAL
FINANCIAL SERVICES ISAC
LEVEL 1
HEALTH ISAC
LEVEL 1
FIRST OBSERVER
IT ISAC
LEVEL 1
MARITIME SECURITY COUNCIL
LEVEL 1
MULTI-STATE ISAC
NORMAL
NEI
NORMAL
APTA
NORMAL
Real Estate ISAC
REN-ISAC
NORMAL
SC ISAC
ST-ISAC
CHEMICAL SCC
OIL AND NATURAL GAS
PCIS
RCCC

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

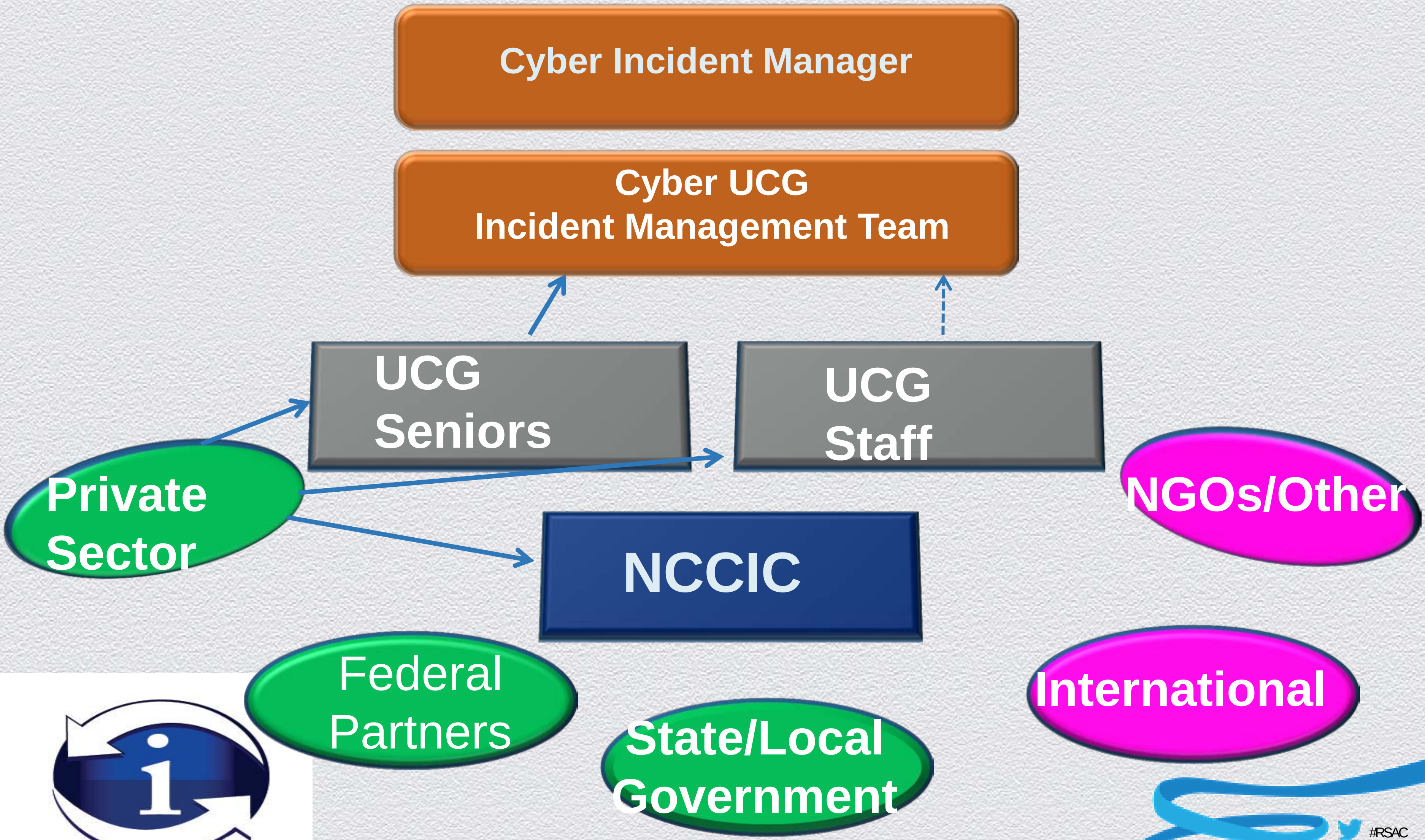
The Public/Private Partnership

How We Work Together

Points of Engagement

- National Cybersecurity and Communications Integration Center (NCCIC)
  - DHS-led Unified Operations Watch & Warning Center
  - Operates 24 hours/day, 7 days/week, 365 days a year
- Unified Command Group-composed of private and public sector representatives
  - Meet monthly and during an incident as needed
  - Advise Assistant Secretary of CS&C on cybersecurity matters, provide subject matter expertise and response as necessary during an incident that requires national coordination

Cyber Incident Response



Cyber Incident Manager

Cyber UCG
Incident Management Team

UCG
Seniors

UCG
Staff

Private
Sector

NCCIC

NGOs/Other

Federal
Partners

State/Local
Government

International

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Case Studies

Physical and Cyber

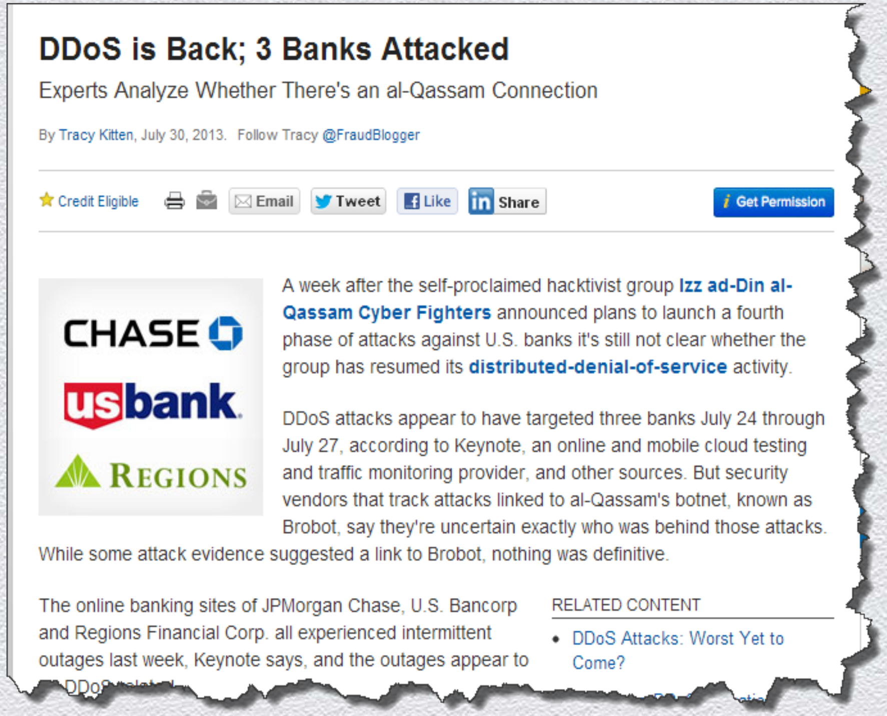
Case Studies

- Hurricanes

NOAA: Sandy Approaching US Coast

Case Studies

POS/Heartbleed/DDoS



DDoS is Back; 3 Banks Attacked

Experts Analyze Whether There's an al-Qassam Connection

By Tracy Kitten, July 30, 2013. Follow Tracy @FraudBlogger

A week after the self-proclaimed hacktivist group **Izz ad-Din al-Qassam Cyber Fighters** announced plans to launch a fourth phase of attacks against U.S. banks it's still not clear whether the group has resumed its **distributed-denial-of-service** activity.

DDoS attacks appear to have targeted three banks July 24 through July 27, according to Keynote, an online and mobile cloud testing and traffic monitoring provider, and other sources. But security vendors that track attacks linked to al-Qassam's botnet, known as Brobot, say they're uncertain exactly who was behind those attacks. While some attack evidence suggested a link to Brobot, nothing was definitive.

The online banking sites of JPMorgan Chase, U.S. Bancorp and Regions Financial Corp. all experienced intermittent outages last week, Keynote says, and the outages appear to DDoS-related.

RELATED CONTENT

- DDoS Attacks: Worst Yet to Come?

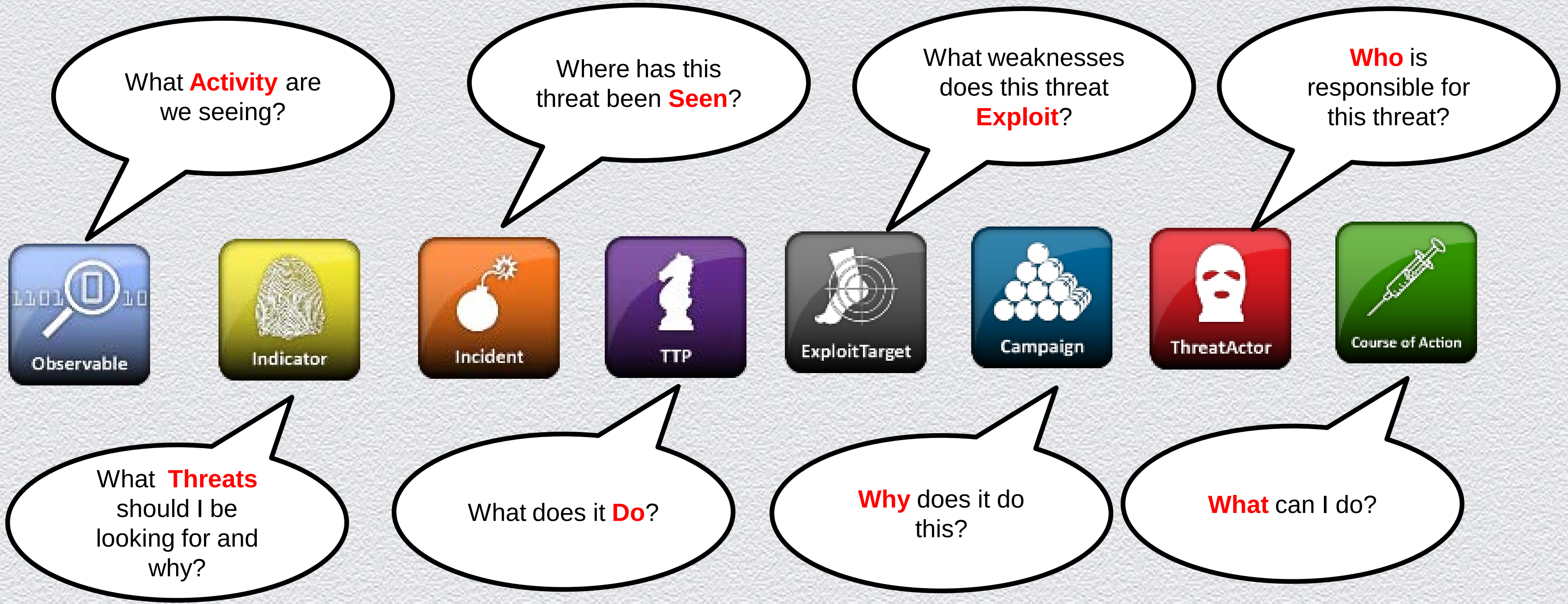
RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Security Automation

The Future of Sharing

Cyber Threat Intelligence

Consider These Questions…..



What **Activity** are we seeing?

What **Threats** should I be looking for and why?

Where has this threat been **Seen**?

What does it **Do**?

What weaknesses does this threat **Exploit**?

Why does it do this?

Who is responsible for this threat?

What can I do?

What Machines See

```
- <cybox:Observable id="fireeye:obser -10fb-4b00-8a49-deb38e92e108">
  <cybox:Title>Mutex: 8ju6thdgf</cyb
- <cybox:Object id="fireeye:object-363 9bd-9163-55378a0fa666">
- <cybox:Properties xsi:type="MutexObj:MutexObjectType">
  <MutexObj:Name condition="Equals">8ju6thdgf</MutexObj:Name>
  </cybox:Properties>
  </cybox:Object>
  </cybox:Observable>
```

```
- <cybox:Observable id="fireeye:observable-42f1ec7e-2a32-4f
fbcb6288c8c9">
  <cybox:Title>Domain: www.dhcpserver.ns01.us</cybox:Title>
- <cybox:Object id="fireeye:object-07e2d2f3-092d-436d-bbd6-60d2bdc36d43">
- <cybox:Properties type="FQDN"
xsi:type="DomainNameObj:DomainNameObjectType">
  <DomainNameObj:Value
condition="Equals">www.dhcpserver.ns01.us</DomainNameObj:Value>
```

```
<stix:Courses_Of_Action>
- <stix:Course_Of_Action timestamp="2014-02-20T09:00:00.000000Z"
id="fireeye:courseofaction-70b3d5f6-374b-4488-8688-729b6eedac5b"
xsi:type="coa:CourseOfActionType">
  <coa:Title>Analyze with FireEye Calamine To >
  <coa:Description>Calamine is a set of free too nizations detect
and examine Poison Ivy infections on their sy kage includes
these components: * PIVY callback-decoding too odule, available
here: https://github.com/fireeye/chopshop) y-decoding tool
(PIVY PyCommand script, available here:
https://github.com/fireeye/pycommands)</coa:Description>
  </stix:Course_Of_Action>
  </stix:Courses_Of_Action>
```

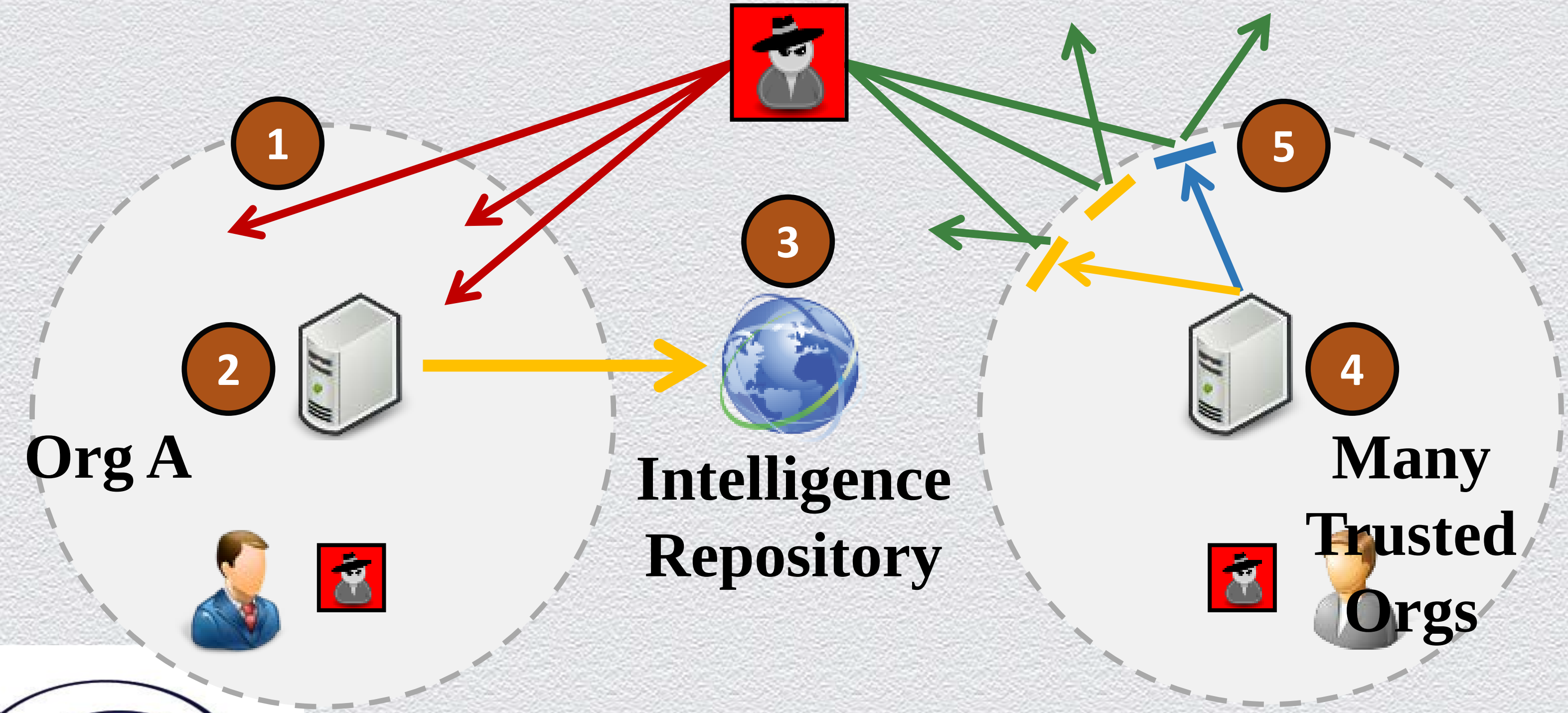
```
- <stix:TTP timestamp="2014-02-20T09:00:00.00 eye:ttp-
aedd016d-12c0-4d6e-902e-9a1cefd3e7e6" xsi:ty pe">
  <ttp:Title>Victim Targeting: th3bug</ttp:Title>
- <ttp:Victim_Targeting>
- <ttp:Identity id="fireeye:ciqidentity30instance-917ed96c-05c2-4754-aed9-
9123341f7cb8" xsi:type="stixCiqIdentity:CIQIdentity3.0InstanceType">
- <stixCiqIdentity:S
  <xpil:Organisation yType="Healthcare Sector,Higher Education
Sector" />
  </stixCiqIdentity:
  </ttp:Identity>
  </ttp:Victim_Targ
  </stix:TTP>
```

```
<stix:TTP timestamp="2014-02-20T09:00:00.000000Z" id="fireeye:ttp-
fb6aa549-c94a-4e45-b4fd-7e32602dad85" xsi:type="ttp:TTPType">
  <ttp:Title>Spear Phishing Attack Pattern as practiced by
menupass</ttp:Title>
- <ttp:Behavior>
- <ttp:Attack_Patterns>
- <ttp:Attack_Pattern capec_id="CA
  <ttp:Description>menuPass app ear phishing to deliver
payloads to the intended targets ckers behind menuPass have
used other RATs in their campaig at they use PIVY as their
primary persistence mechanism. >
  </ttp:Attack_Pattern>
  </ttp:Attack_Patterns>
  </ttp:Behavior>
```

The underlying data shared in a language called Structured Threat Information eXpression or STIX

Sharing Solution

- **Instead of 2% or less of attacks blocked, detected, or prevented, a much higher percentage of attacks are stopped**



Current Status

- Pilot group aka “Friends and Family”
  - 25 Organizations Participating
- Vision Gaining Momentum
  - Live at NH-ISAC
  - Working with several others
- Released Version 1.2 to the group
  - Focus on “installability”
- Enabled Collaboration
  - Forums, Bug Tracker, Download System
- Conversion of Open Source Intel Feeds
  - Approximately 14 sources

Road Map

- May 12th - Avalanche 1.3
  - Peer 2 Peer
  - Super fast TAXII Service
  - GUI Indicator Builder
- June 30th – Avalanche 1.4
  - STIX Enhancements
  - Trust Groups
  - Peer 2 Peer changes
- July 31st – Avalanche 1.5
  - Adapters
  - Trust Group Changes

- August 28th – General Availability

Questions?