An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

HIS Conference
Sligo
Thursday 31st Match 2022

Agenda

- ❑ NCSC overview
- ❑ What are ISAC's
- ❑ ISAC models
- ❑ Examples of ISACs
- ❑ Benefits of ISACs
- ❑ References

NCSC Roles Responsibilities

Incident Response

- Lead national response to major cyber security incidents

Resilience

- Building capacity and resilience

Information Sharing and Support

- Enhance situational awareness amongst constituents and the general public in regard to relevant cyber security threats

Operational Tasks

Notification

- Victims
- Constituents
- General Public
- Partners

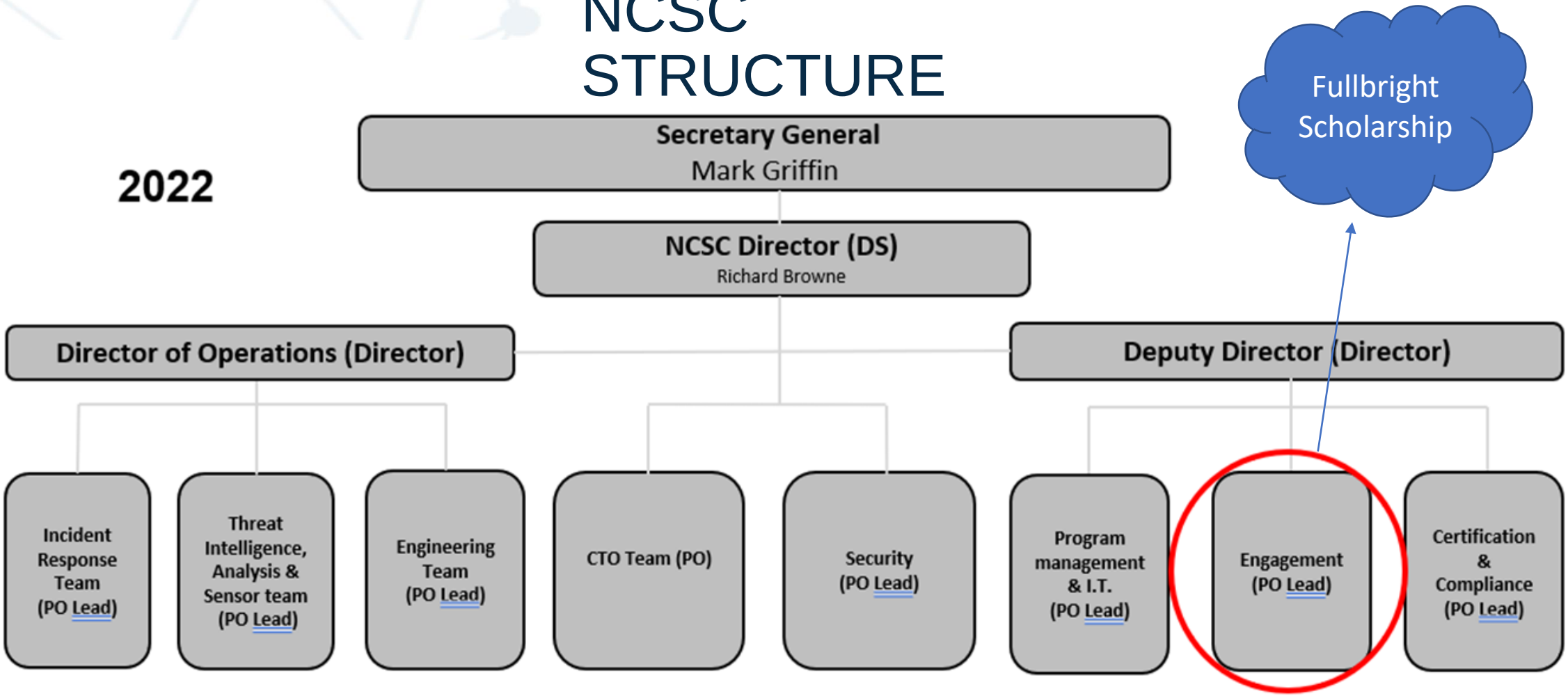
Analysis

- Malware
- Forensics
- Email
- Threat Actor Groups

Monitoring

- Threat Intel Database
- External Channels
- Partner Orgs

NCSC STRUCTURE



- Cyber Security Baseline Standards

https://assets.gov.ie/205834/1727388a-02d6-47d4-bebe-38774da2f321.pdf

NIS Compliance Guidelines for OES

https://assets.gov.ie/76729/ea0bcd3b-0161-41d2-8c51-df00e558689c.pdf

NCSC NL – Benefit more from your ISAC

https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2020/february/24/a-practical-guide-benefit-more-from-your-isac/200206+NCSC+Next+Gen+ISACs+EN+A4+web.pdf

Includes a checklist to determine ISAC Level for each capability:

- strategy and action plan
- working method
- information structure and information management
- situational awareness and lessons learned
- action

What are ISACs:

Information Sharing and Analysis Centres

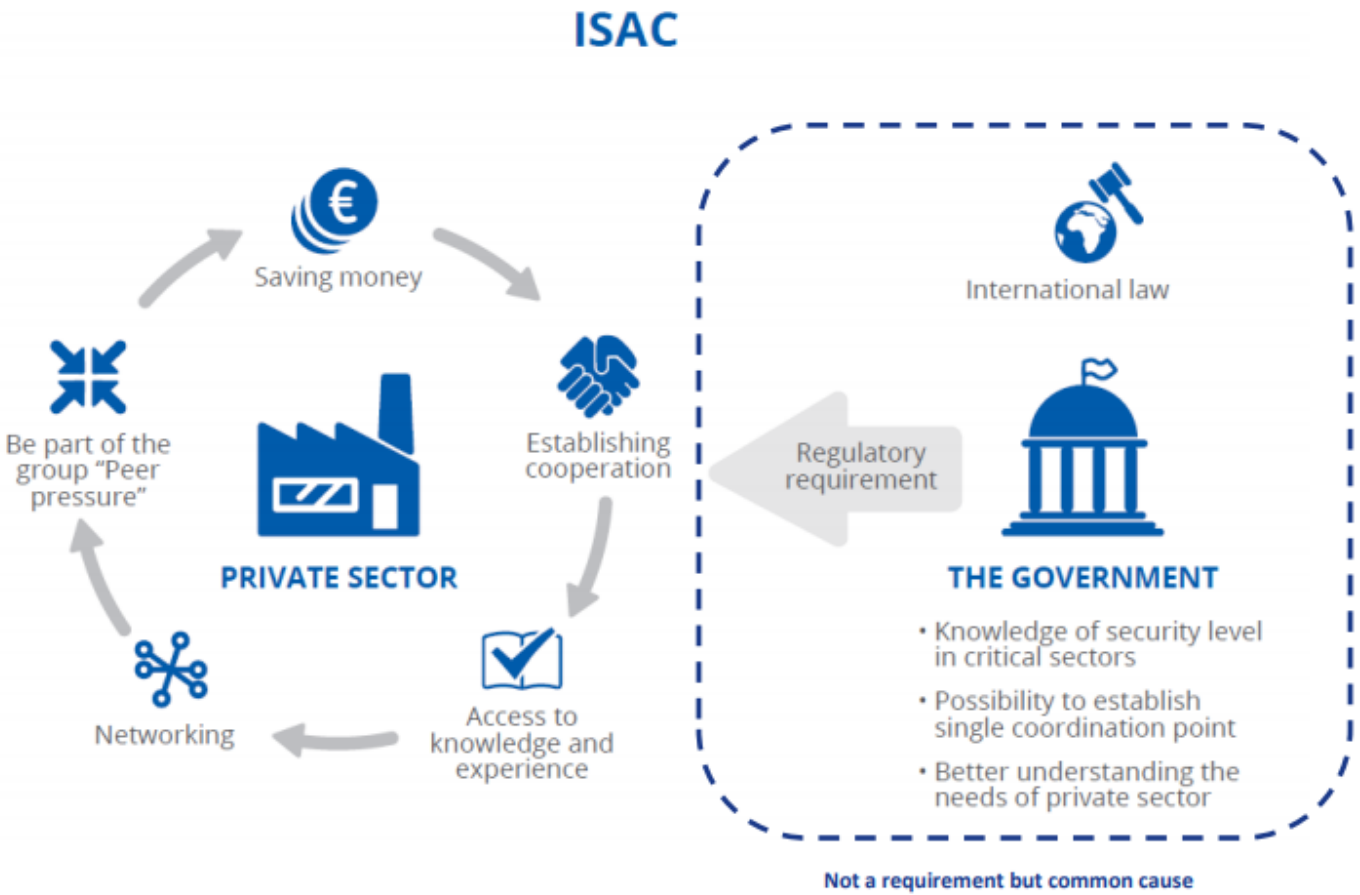


Figure 1: Reasons for the creation of ISACs

Types of ISACs

ENISA
Information Sharing and Analysis Centres (ISACs) models

- ❑ Country Focused
- ❑ Sector Specific
- ❑ International ISACs

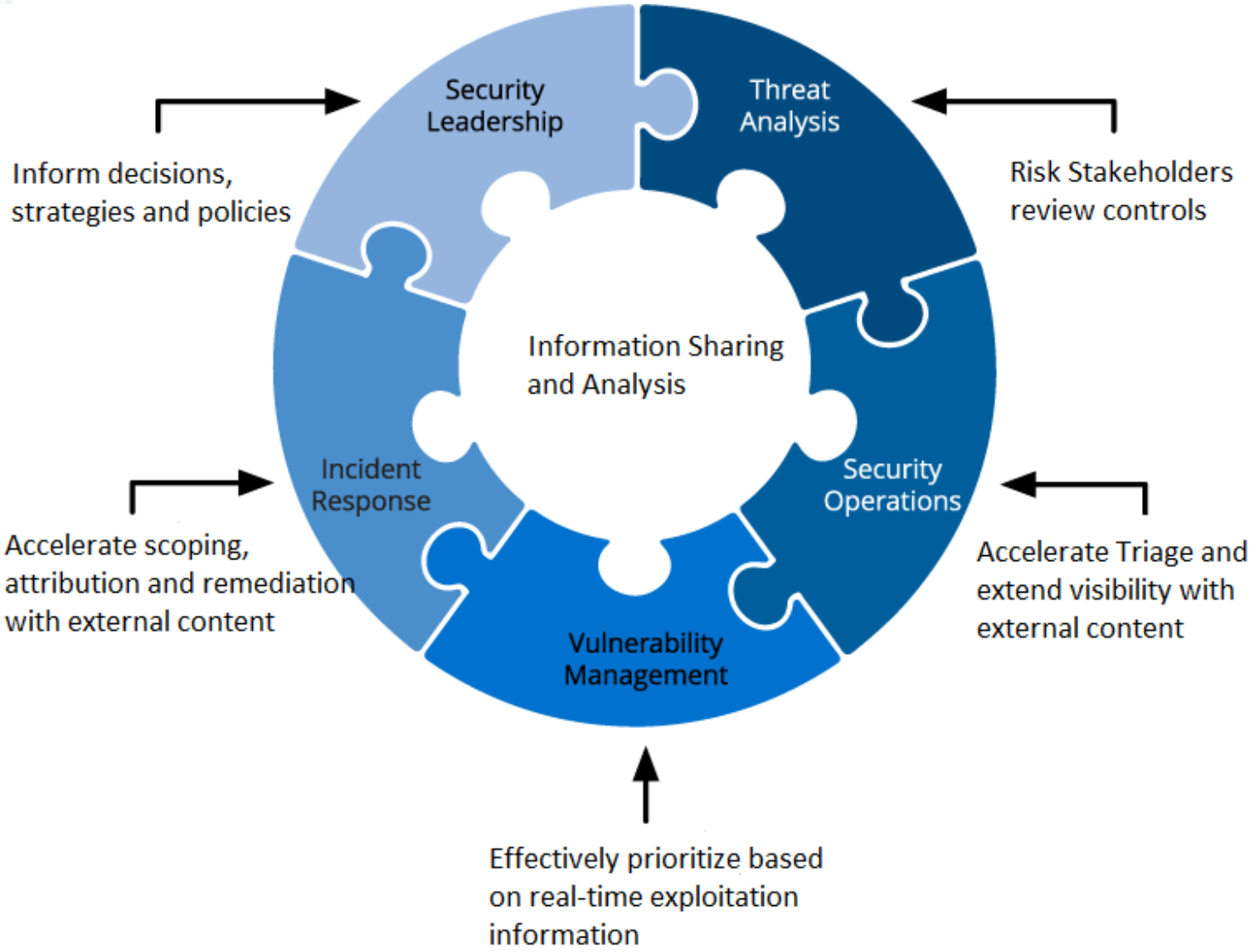
Examples of sectors that have created ISACs:

- Financial

- Energy

- Aviation

Benefits of ISACs



Challenges with ISACs

Building trust

Securely share information between organisations with different levels of cybersecurity maturity

Chinese walls

Ensure sharing does not impact compliance or law enforcement

Start slow

Build trust, define ToR, outline roles, responsibilities, information sharing protocols, establish links with other ISACs

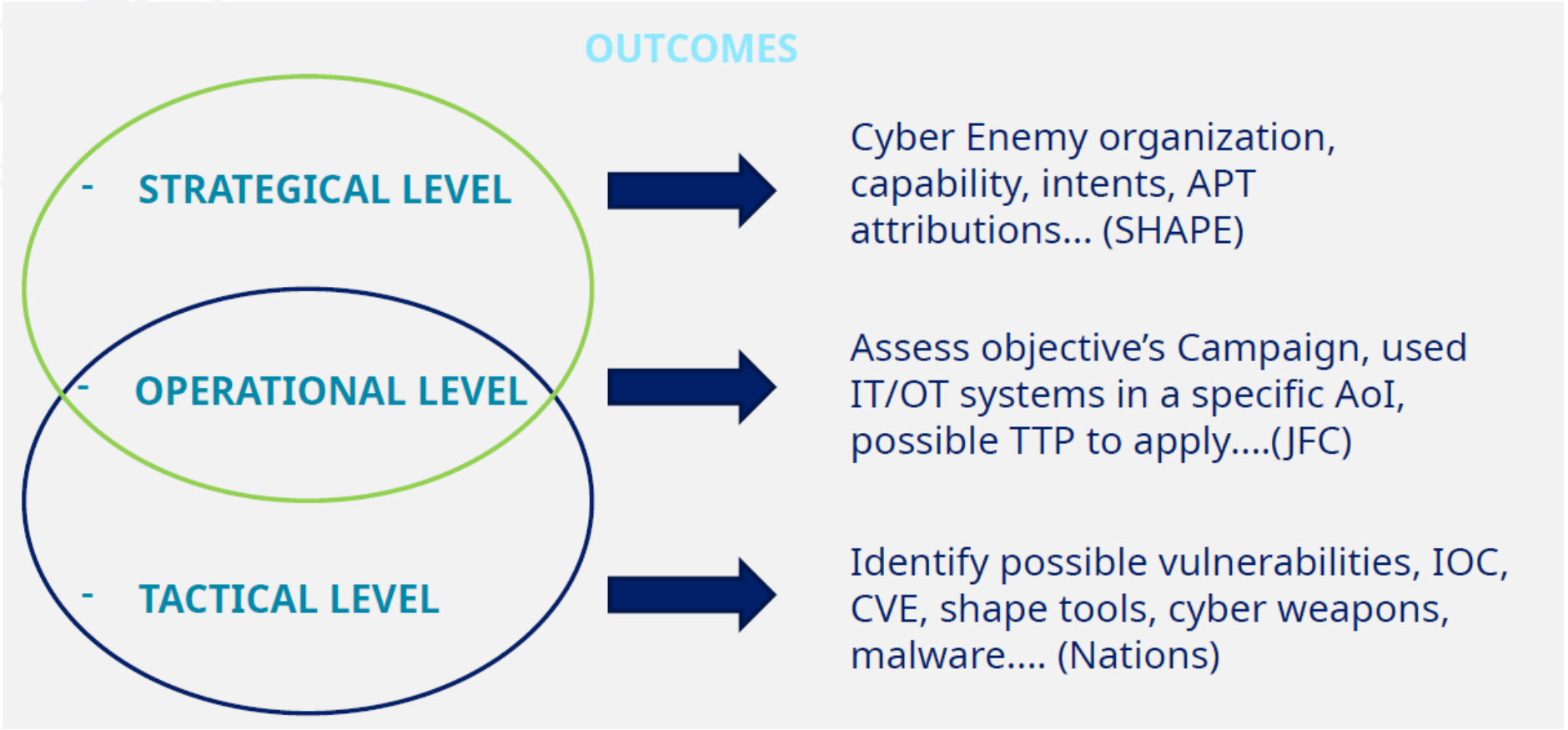
Bottom up

Commission advocates a voluntary bottom up approach, rather than through Directives

Different perspectives

Source: https://forums.soltra.com/index.php?/topic/266-soltra-intro-pdf-deck/

Different perspectives



NIST Cyber Security Framework

	Function
What processes and assets need protection?	Identify
What safeguards are available?	Protect
What techniques can identify incidents?	Detect
What techniques can contain impacts of incidents?	Respond
What techniques can restore capabilities?	Recover

- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

NIST CSF

IDENTIFY

Risk Assessment (ID.RA):
Cybersecurity risk to organisational operations, assets, and individuals are identified and understood.

ID.RA-2:
Cyber threat (strategic, operational and tactical) and vulnerability information is received from information sharing forums and sources.

ID.RA-3:
Threats, both internal and external, are identified and documented.

ID.RA-5:
Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. Risk assessments are dynamic and are updated in light of system or service changes, or changes to the threat environment.

ENISA

ENISA
Information Sharing and Analysis Centres (ISACs) models and good practice

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

NIST
SP 800-150, Guide to Cyber Threat Information Sharing
Guidelines for establishing and participating in cyber threat information sharing relationships

https://csrc.nist.gov/publications/detail/sp/800-150/final

NIST SP 800-53 R4

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
Control: The organization:

- Receives /Disseminates information system security alerts, advisories, and directives to/from [Assignment: organization-defined external organizations] on an ongoing basis

PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:

- security education and training
- maintain currency with recommended security practices
- share current security-related information

Q & A