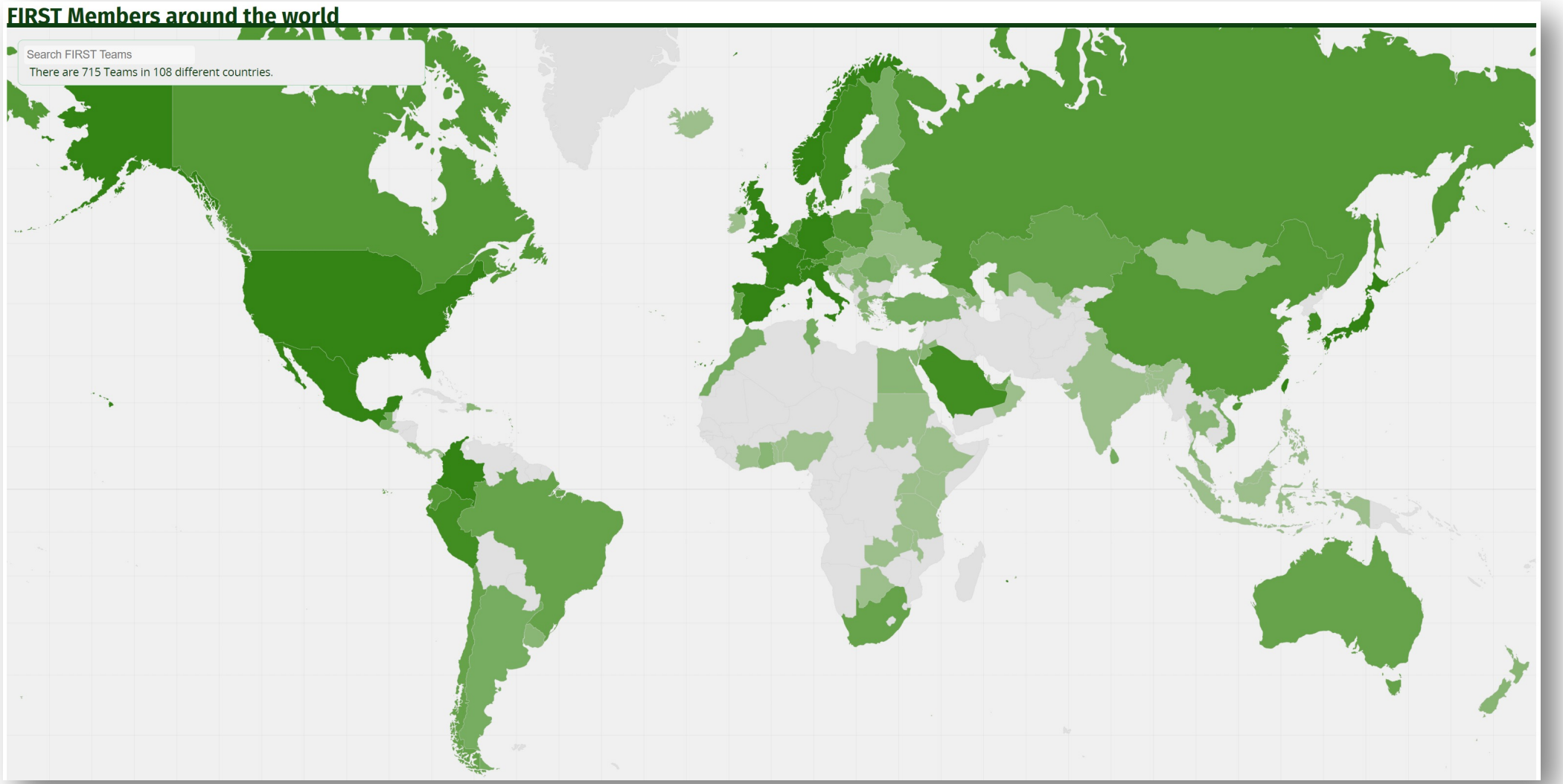


ITU-T SG17 Mini Workshop on ITU-T X.1060: Exploring an Operational Framework for Cybersecurity, 2024-02-22, Geneva

Session 2: Enhancing collaboration on major operational frameworks for cybersecurity:

Vilius Benetis, https://www.linkedin.com/in/viliusbenetis/

Contributor to the FIRST CSIRT Service Framework | Director, NRD Cyber Security, Lithuania

For those who do not know what FIRST.org is:

FIRST Vision and Mission Statement

Vision

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all.

Effective response is a global task, mirroring the global nature of the internet. Based on a peer to peer network governance model, Computer Security Incident Response Teams (CSIRTs), Product Security Incident Response Teams (PSIRTs) and independent security researchers work together to limit the damage of security incidents. This requires a high level of trust; the fuel our members run on. FIRST fosters trust building among members through a variety of activities. Incidents are not confined to one cultural or political corner of the internet, nor do they respect borders or boundaries. FIRST thus promotes inclusiveness, inviting membership from all geographic and cultural regions.

Missions

Global Coordination - You can always find the team and information you need.

FIRST provides platforms, means and tools for incident responders to always find the right partner and to collaborate efficiently. This implies that FIRST's reach is global. We aspire to have members from every country and culture.

Global Language - Incident responders around the world speak the same language and understand each other's intents and methods.

During an incident it is important that people have a common understanding and enough maturity to react in a fast and efficient manner. FIRST supports teams through training opportunities to grow and mature. FIRST also supports initiatives to develop common means of data transfer to enable machine to machine communication.

Policy and Governance - Make sure others understand what we do, and enable us rather than limit us.

FIRST members do not work in isolation, but are part of a larger system. FIRST engages with relevant stakeholders, in technical and non-technical communities, to ensure teams can work in an environment that is conducive to their goals.

History

- Originally adopted by the FIRST Steering Committee, 11 January 1995.*
- Amended during the FIRST Annual General Meeting, 26 June 1997.*
- Re-drafted by the FIRST Steering Committee, March 2003, and approved by the FIRST Annual General Meeting, 26 June 2003.*
- Adopted by the FIRST Board, July 2020

https://www.first.org/standards/frameworks/

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog

Standards & Publications
- Standards
- Publications
- Best Practices Guide (BPGL)
- Security Reference Index

Standards
- Common Vulnerability Scoring System (CVSS-SIG)
- Traffic Light Protocol (TLP)
- Service Frameworks
- Information Exchange Policy (IEP)
- Passive DNS Exchange
- Exploit Prediction Scoring System (EPSS)

Service Frameworks
- CSIRT Services Framework
- PSIRT Services Framework

FIRST Services Framew

The *Services Frameworks* are high level docu
community. FIRST strives to include feedbac
These documents where intended to provide a foundation for the developmen
defining an initial service catalogue for new teams. These documents will be m
nese, French, Russian and Spanish.

In the creation of the CSIRT framework it became clear, that PSIRTs do provide
to create a separate document covering PSIRTs. The two documents will be alig

The development of the Frameworks is driven by the CSIRT Framework Development SIG.

Purpose

PSIRT Services Framework

English
- PSIRT Maturity, HTML
- PSIRT Maturity, PDF Format
- v1.1 HTML
- v1.1 PDF Format
- v1.0 HTML
- v1.0 PDF Format

Arabic
- v1.1 PDF Format

Chinese
- v1.1 PDF Format

French
- v1.1 PDF Format

Spanish
- v1.1 PDF Format

Japanese
- PSIRT Maturity, PDF Format
- v1.0 PDF Format

Russian
- v1.1 PDF Format

CSIRT Services Framework

English
- v2.1 HTML
- v2.1 PDF Format
- v2.0 PDF Format
- v1.1.1 PDF Format
- v1.1 PDF Format

Arabic
- v2.1 PDF Format

Chinese
- v2.1 PDF Format

French
- v2.1 PDF Format

Spanish
- v2.1 PDF Format

Japanese
- v1.1 PDF Format
- v2.1 PDF Format

Russian
- v2.1 PDF Format

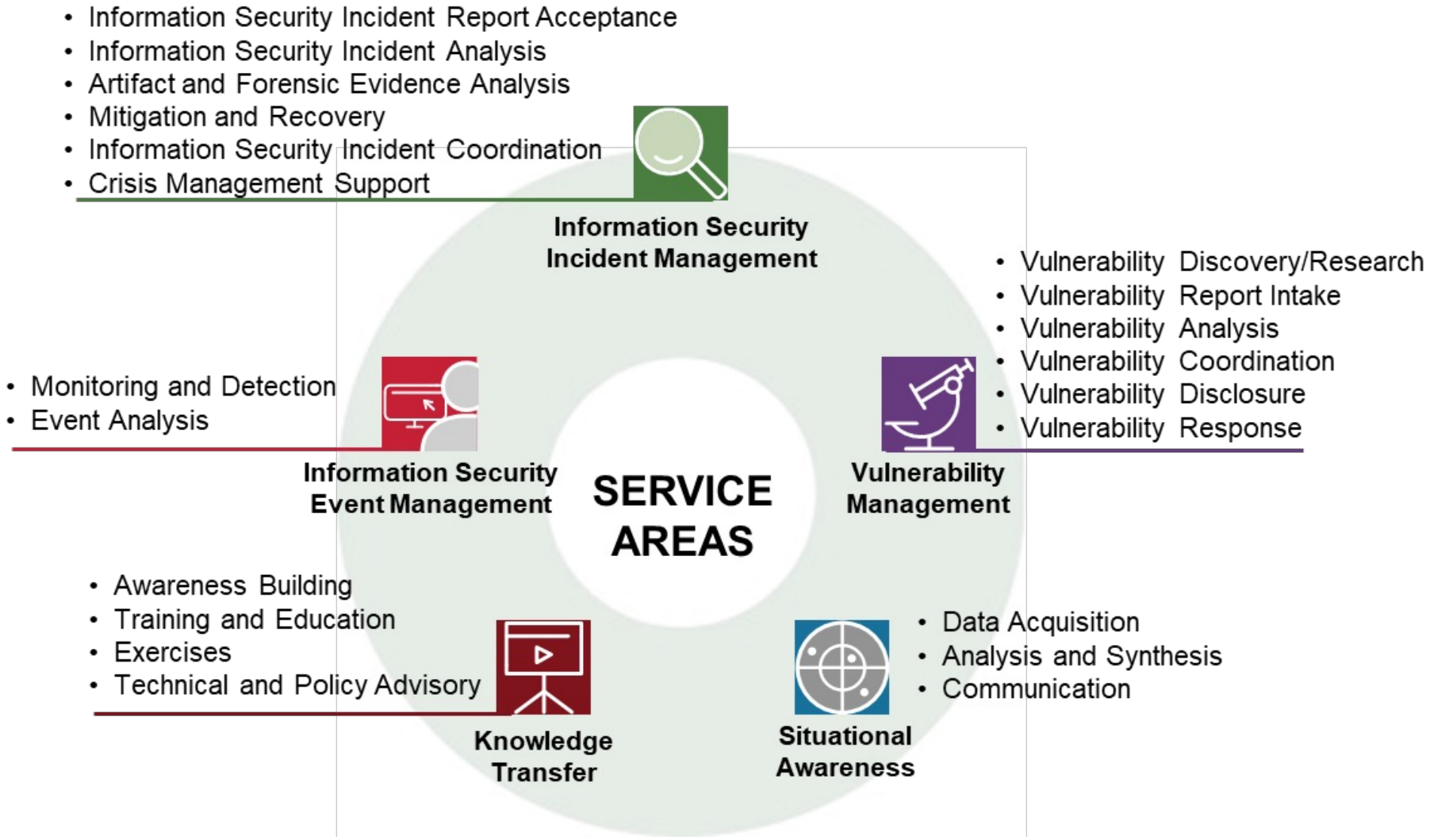
Addendum

CSIRT Roles and Competencies
- v0.9.0 PDF Format -

New Document

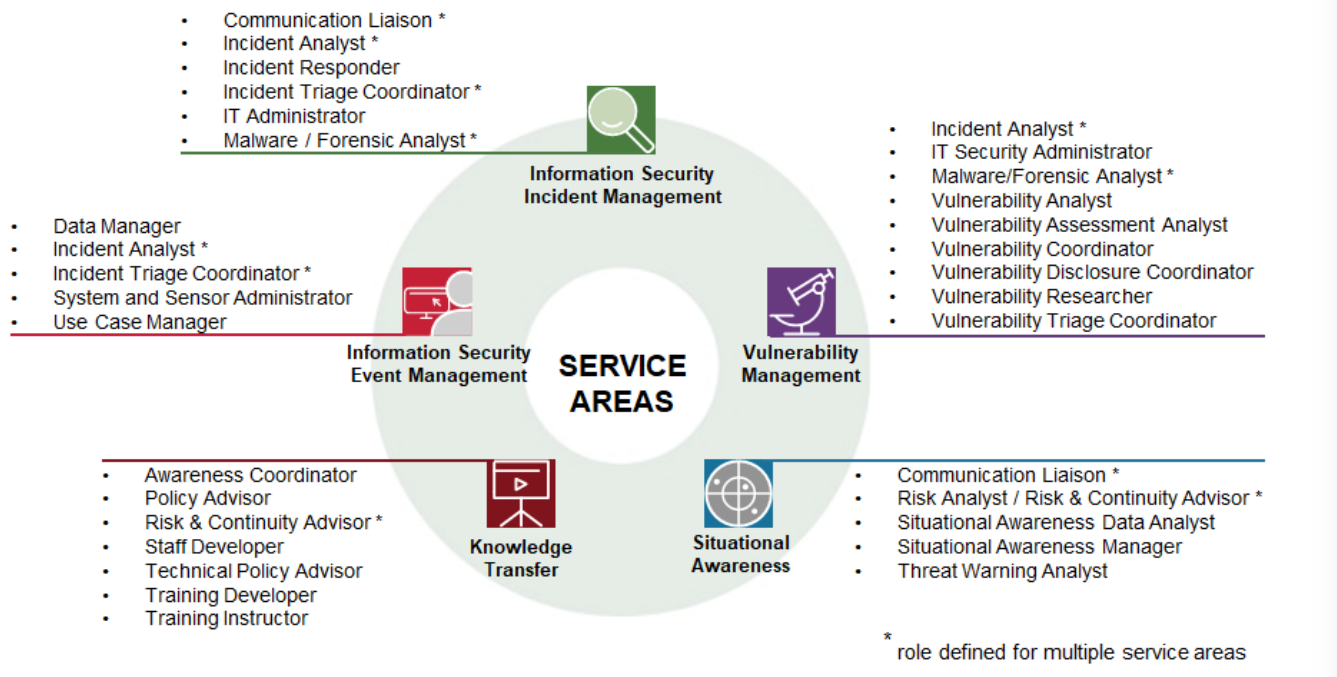
Incident Management Team Types
- v0.7.1 PDF Format

Clear Information Security Incident Governance Model:
FIRST.org Services Model Framework



https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

FIRST.org CSIRT Services Roles and Competences v0.9
(CSIRT SIG, 76p report)



URL: https://www.first.org/global/sigs/csirt/

5.2.2 General Tasks

- Analyze and understand information security events, potential and confirmed information security incidents
- Assess the potential and actual impacts and damages
- Analyze incidents to identify root cause and impact
- Conduct cross-incidents analysis
- Analyze media and perform surface analysis of artifacts
- Discover incident-related vulnerabilities used by attacks
- Identify and correlate, when appropriate, distinct but possibly related security events and/or incidents to better understand the context of the incident in a bigger picture

5.2.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Event Management
  - Event Analysis
    - Correlation (5.2.1)
- Service Area: Information Security Incident Management
  - Information Security Incident Report Acceptance:
    - Information Security Incident Root Cause Analysis (6.2.4)
    - Cross-Incident Correlation (6.2.5)
  - Artifact and Forensic Evidence Analysis:
    - Media or Surface Analysis (6.3.1)
- Service Area: Vulnerability Management
  - Vulnerability Discovery/Research:
    - Incident Response Vulnerability Discovery (7.1.1)

5.2.4 Generic Competencies

- Professional
  - Conflict Management (C009)
  - Critical Thinking (C011)
  - Oral Communication (C036)
  - Written Communication (C060)
- Technical
  - Problem Solving (C040)

5.2.5 Role-Specific Competencies

- Operational
  - Data Privacy and Protection (C014)
  - External Awareness (C019)
  - Legal, Government, and Jurisprudence (C030)
  - Organizational Awareness (C037)
- Technical
  - Computer Forensics (C005)

FIRST Services Framework:

Team Types Within the Context of Services Frameworks

Version 0.7.1 Review

Document URL:

https://www.first.org/standards/frameworks/csirts/team-type

Work continues:

1. Analyzing subtypes in CSIRT, ISAC, SOC, PSIRT
2. OCF SIM3 adjustment to the types

Service Area	SOC	CSIRT	PSIRT	ISAC
Information Security Event Management				
Monitoring and Detection	MUST	-	-	-
Event Analysis	MUST	-	-	-
Information Security Incident Management				
Information Security Incident Report Acceptance	-	MUST	-	-
Information Security Incident Analysis	-	MUST	-	-
Artifact and Forensic Evidence Analysis	-	-	-	-
Mitigation and Recovery	-	MUST	-	-
Information Security Incident Coordination	-	MUST	-	-
Crisis Management Support	-	-	-	-
Vulnerability Management				
Vulnerability Discovery/Research	-	-	-	-
Vulnerability Report Intake	-	-	MUST	-
Vulnerability Analysis	-	-	MUST	-
Vulnerability Coordination	-	-	MUST	-
Vulnerability Disclosure	-	-	MUST	-
Vulnerability Response	-	-	MUST	-
Situational Awareness				
Data Acquisition	-	-	-	MUST
Analysis and Synthesis	-	-	-	MUST
Communication	-	-	-	MUST
Knowledge Transfer				
Awareness Building	-	-	-	-
Training and Education	-	-	-	-
Exercises	-	-	-	-
Technical and Policy Advisory	-	-	-	-

Cooperation with X.1060

- Interest to align / remove conflicts of terms and concepts
- Make standards supporting each other (via references, via aligned structures, clarifications on how additional value is added)