FIRST™

DECEMBER 7-9, 2021

2021 VIRTUAL SYMPOSIUM

AFRICAN AND ARAB REGIONS

Co-hosted by

AfricaCERT

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT

Pete Allor, Red Hat
Josh Dembling, Intel

PSIRT SIG Co-Chairs

December 7, 2021

Translation services provided by

Internet Society

WWW.FIRST.ORG

Our History

- Formed 8 years ago to create the PSIRT Services Framework
- We have ~100 individuals from 44 companies (22 / 9)
- Conducted the 6th Annual FIRST PSIRT TC – and first hybrid TC (2020)
- Delivered PSIRT Services Framework v1.0 2017; v1.1 2019
- Produced Overview PSIRT Training Videos and Maturity Guide 2018
- Enable the Exchanged Best Practices between PSIRT participants
- Developing the PSIRT Common Body of Knowledge

Our Mission

The PSIRT SIG is an assembly of **active industry practitioners** driving the evolution of PSIRT practices by developing and maturing product security response, through **collaborating** to bridge the knowledge gap between vulnerability and response aspects of product security from newly formed to well-established teams

The SIG will **educate and inform PSIRTs on known good practices**, continue the development of the PSIRT Services Framework, curate and develop supporting training materials, and empower them to rapidly address the evolving threat landscape

Goals and Deliverables

- Foster collaboration between PSIRTs across different organizational and industry verticals
- Develop and share a common body of knowledge (CBK) on PSIRT best practices
- Produce PSIRT-focused collateral to assist in educating corporate leadership
- Curate a list of all PSIRT-focused conferences and colloquia
- Publish a PSIRT capability maturity assessment
- Provide online education and training materials to PSIRTs of various maturity levels
  - Publish PSIRT Education topics on the FIRST website under a creative commons license
  - Organized by topic (Intro, Process, Consuming), Response, Scoring, Tooling, Support)
  - Reach a wide audience (Baseline, Company, PSIRT Ops, PSIRT Leadership/Management, QA, Security Officers, Security Engineers)
  - The content will align to the PSIRT Framework and terminolog

Working Groups

The SIG has operated now for the past seven years continuously and prior to moving into our regular working groups, collectively met bi-weekly with about 20 sessions per year plus a three day in-person TC, with a workshop and the Annual Conference for an additional face-to-face

We are moving from five to three Working Groups:

- Framework 2.0, Maturity and Supporting Documentation
- PSIRT Tooling and Third Party Components - Product Incident Response Orchestration Needs, Expand a platform like VINCE to meet needs of Vendor Community, Third Party Component issues that feed manifest and into SBOMs
- Incident Coordination Working Group- Group response and preorganized multiparty approaches; Develop a common set of needs to allow groups to coordinate response together
    - ICASI and other like Groups
    - Affinity Groups

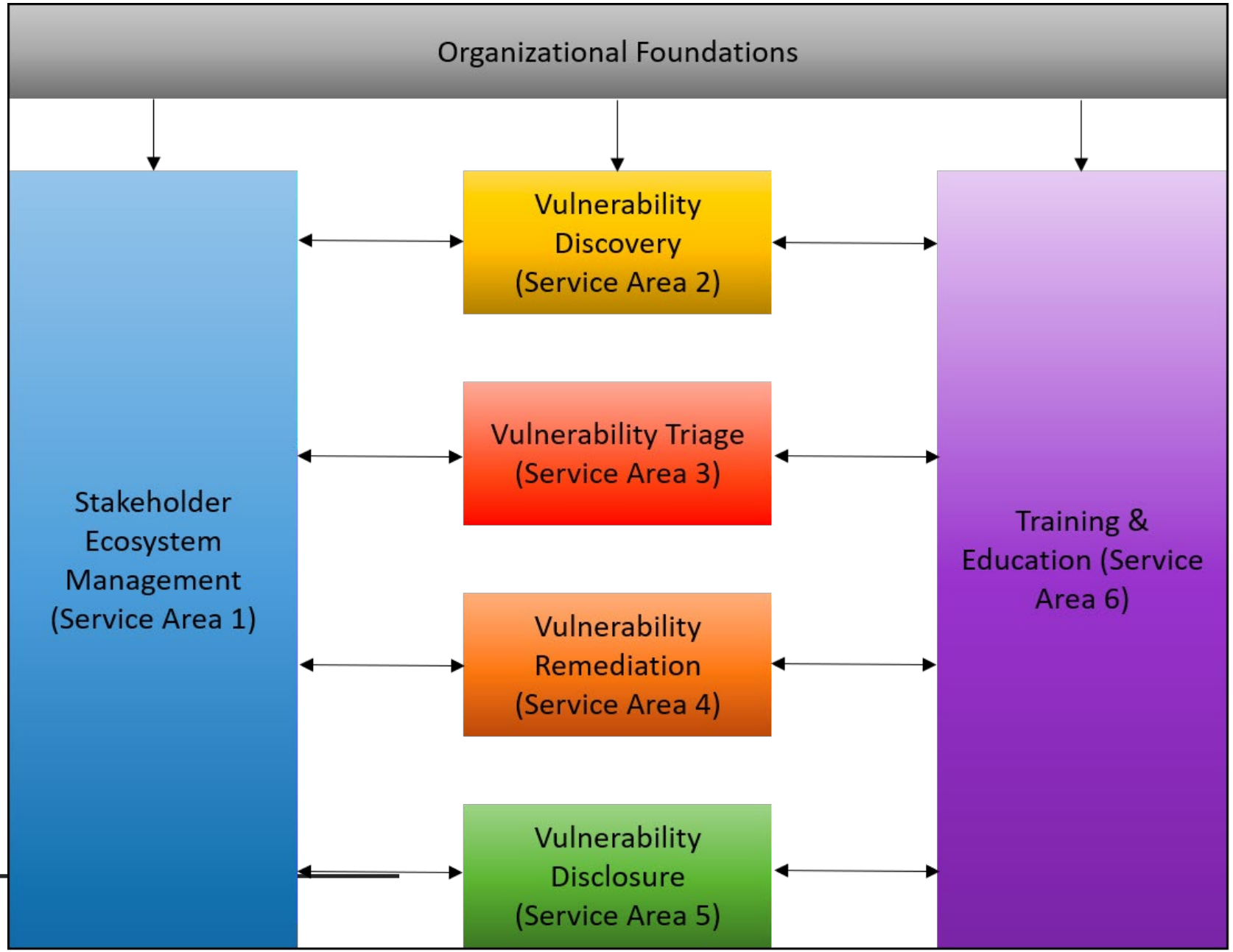
PSIRT Document Layers

- Layer 1 - PSIRT Services Framework
  - V1.0
  - v1.2
  - v1.x (~Q2 2022)
- Layer 2 - Levels of Maturity
  - Simple
  - Complex
- Layer 3 - Supporting Documentation
  - Incident Response Plan (~Jan 2022)

Formation of PSIRT Services Framework

- Initial work in 2015, drafting in earnest in 2016 after reviewing CSIRT Services Framework
- FIRST PSIRT TC February 2015
- Version 1.0 published June 2018
- Version 1.2 updated June 2020 and translated by ITU Spring of 2020
- PSIRT TC 2020 drew over 100 participants from 60+ organizations
- Collaborative work of 40+ active PSIRTs globally
- Based on practical application and best practices

PSIRT Services Framework



Why Maturity and Supporting Documents

- Framework is a starting point for of a full range of potential services that a PSIRT could select from. They are guiding elements for design and functionality of a PSIRT to work with your corporate leadership and designed for consideration of what your stakeholders want.
- Maturity documentation is a means by which a PSIRT can repeatedly measure themselves against in a consistent manner. This body of knowledge will grow over time and is meant as a guideline, not a checklist
- Supporting documentation is meant as primers and how to's and are from practicing PSIRTs as a means to 'jump' start others to move beyond initial practices and hopefully to have a smaller learning curve

Our Future

- Does your organization write and distribute apps?
- Are you producing code and putting it out for customers?
- If you are, you have crossed into needing to run PSIRT Operations.
- Doing PSIRT ops well, come share your practices and challenges
- Members of PSIRTs come join us!

Copyright