PSIRT Framework

Service Area 1

Stakeholder Ecosystem Management

Key Concepts

What is a Stakeholder and why are they important?

- Service Area 1 deals with stakeholders. A stakeholder is a someone that has a vested interest in the capabilities and services the PSIRT offers.
- Each stakeholder group will have their own unique viewpoints (perspective) that will require the PSIRT to deliver views (artifacts) to satisfy.
- Stakeholders can be customers, executives, partners, and peers. Anyone that needs or wants something from the PSIRT is some form of a stakeholder.

Service Area 1 Purpose & Outcomes

- **Purpose** – Highlight the processes and mechanisms to share information with assorted stakeholders a PSIRT can and should interact with.
- **Outcome** – Successful engagement with the PSIRT's stakeholder ecosystem will ensure timely reports of discovered vulnerabilities as well as satisfied stakeholders/partners when security vulnerabilities must be communicated to the organization's stakeholders.

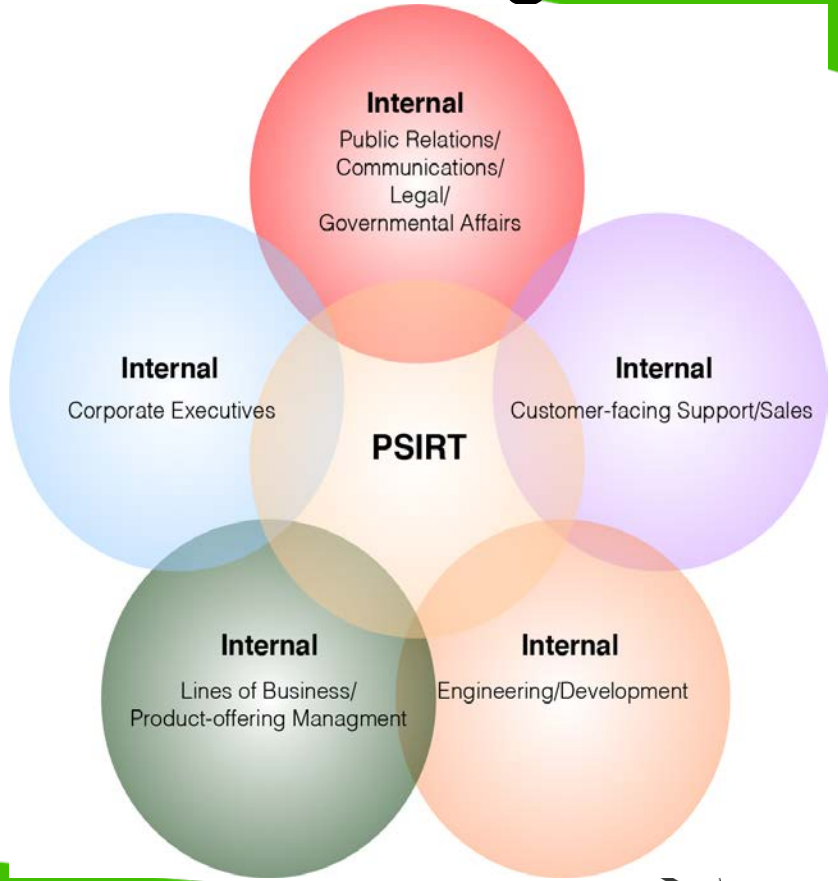
Who are my Stakeholders?

- Different stakeholders will want and need different services or artifacts from the PSIRT
- We can divided up the Stakeholders into generalized groups:
  - Internal
  - Finders (people who report vulnerabilities to the PSIRT)
  - Upstream Communities (Providers or collaborators)
  - Downstream (Partners or consumers)

Internal Stakeholders

Service 1.1 -Internal Stakeholder Management

- Service 1.1 is focused the groups of stakeholders the PSIRT should engage with across their organization.
- These groups typically all will report up to some single executive layer (although not always).
- Here is a sample of the other teams the PSIRT could work with.



What is special about Internal Stakeholders?

- By building relationships with these groups, this assists in working towards the goal of smooth handling of reported vulnerabilities and timely distribution of updates to downstream.
- Some Internal Stakeholders can be supporting functions to the PSIRT (Corporate Communications), while others are critical partners that also work to help protect the company (Legal and/or Public Relations), while others still rely upon the PSIRT's expertise to provide data to support consumers of the organization's products (Sales or Support)

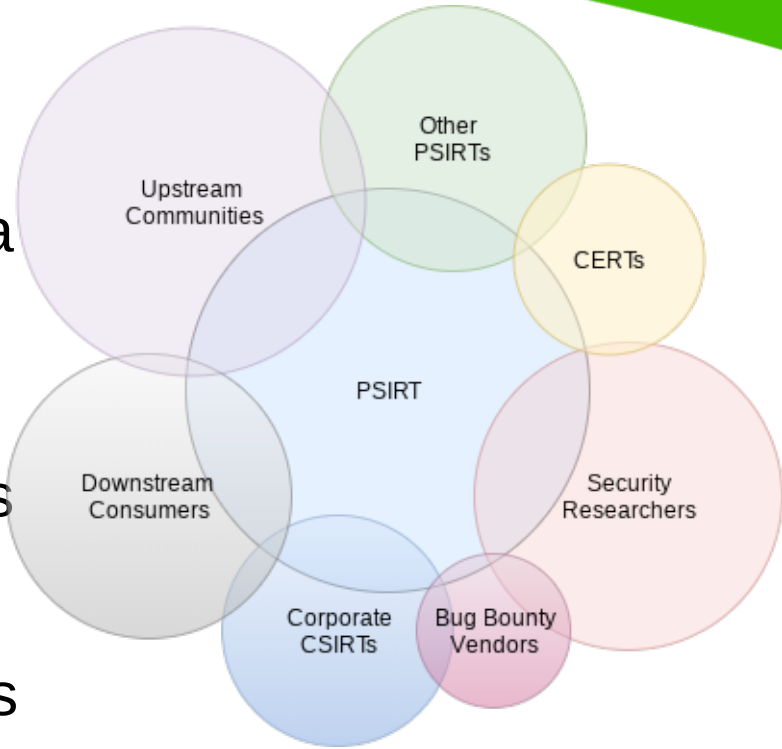
Two things that are better together

- The PSIRT may need to approach each Stakeholder group differently.
  - Corporate Executives want data differently than Engineers, or Support staff.
- Decide which groups have the most immediate needs of the PSIRT and focus on those first.
  - Reports to execs, while nice, may need to for worked on after implementing a workflow with product engineering to actually ingest, prioritize, and deliver vulnerability fixes.
  - Ultimately, all Internal Stakeholders share the goals of making the organization and its products successful; find ways to merge your mission into that larger organizational structure.

Finder Management

Service 1.2 -Finder Community Engagement

- A Finder is a person or group of people that discover a security vulnerability.
- A Finder could be an academic researcher, a professional bug hunter, a security firm, a hobbyist, an industry peer, a customer, or even an employee from the PSIRT's own company.
- Good relationships with these Finders is CRITICAL to the on-going success of the PSIRT.
- This community includes several groups



Other PSIRTS

- Through groups, like FIRST or other channels, the PSIRT will interact with other Product Security Teams.
- Having good relationships with peer PSIRTs can be of great benefit both from the product and professional standpoints.

Coordinators

- Groups like US-CERT or JP-CERT are government-sponsored teams that dedicated to coordinating disclosure around vulnerabilities.
- Working with these groups can help connect the PSIRT to a more global audience.

Security Researchers

- Researchers/Finders are some of the most important relationships to cultivate.
- These typically will be the people finding and reporting many of the vulnerabilities the PSIRT will need to develop fixes for.
- It is important to have easily available and clear reporting guidelines for Finders to review.

Bug Bounty Vendors

- The PSIRT could elect to work with a bug bounty vendor to assist in reporting and/or coordination
- These groups pay Finders rewards for reporting found vulnerabilities to them.

Corporate CSIRTs

- Unlike a technical end-user of the company's products, a CSIRT has a specific security-focused viewpoint and different needs than a standard system administrator.
- Part of the PSIRT's output will need to account for this perspective, and the PSIRT may be occasionally asked to communicate directly with these focused groups.

Community Stakeholder Engagement

Defining your Communities

- Two terms that might be new to the PSIRT:
  - Upstream
  - Downstream

Defining your Communities - Upstream

- An Upstream community is an organization or group that provides materials vital to the PSIRT organization's product
  - Think about open source communities that make modules the product teams use, or a hardware OEM that provides microchips for the company's hardware products.

Defining your Communities - Downstream

- A Downstream community is a group or organization that take your organizations products and services and uses or redistributes them.
  - In open source, your company may maintain and provide drivers for your hardware.
  - Someone may resell your products and come to you for support
  - This also can be considered your customers; users of your company's products.

Working with your Communities

- Each of these stakeholder groups has unique viewpoints and needs from the PSIRT.
- Communication content and channels will be different for each.

Incident Coordination

Why Incident Communications are critical

- As reviewed so far, the PSIRT has many different groups inside and outside of the company they must interact with.
- Each one of these groups wants different things during the normal course of business, and when the PSIRT needs to share information around some type of security incident occurs all of that becomes amplified.
- Clear, professional handling of the distribution of this information helps protect the PSIRT’s customers, and the overall corporate brand of the organization.

Plan the work, work the plan

- The best time to plan for a crisis is when one is not going on. Take times between issues to map out how you need to react for both “normal” security flaws as well as ones that may generate large amounts of media attention.
- Having plans, checklists and templates ahead of time, and having staff trained on what to do will help ensure the company can successfully react as they arise.
- Building those inter-company relationships can help the PSIRT get the appropriate attention and resources to solve a vulnerability and get it delivered quickly to your customers.

Recognition

Acknowledgement, Rewards, and Recognition

- The PSIRT will need to work out how they wish to interact with Finders and the general research community.
- Based off of the industry, there are generally-accepted practices the PSIRT should consider doing for persons reporting issues that get resolved.
- At a minimum, it is general practice to acknowledge the person or organization that discovered and reported the issue in some public forum (public webpage, security advisory, defect tracking system, etc.). Some organizations elect to do more.

Stakeholder Metrics

Who measures the Measuremen?

- To be able to understand if and how well the PSIRT is achieving its mission, metrics will need to be created and shared with stakeholders.
- Each stakeholder will have unique needs from the PSIRT, and may require unique metrics.
- Wherever possible, as the PSIRT deploys process and tooling, statistics should automatically captured to avoid costly manual efforts in the future.

Analysis and Review

- As viewpoints are developed to address each stakeholder's unique views, the PSIRT will need to devote time to understand the data.
- Changes to PSIRT process and interactions may be needed to achieve necessary metrics (which should represent goals the organization desires to achieve).
- This data should be put into context and periodically shared with stakeholders.

In Closing

Copyright