PSIRT Framework

Service Area 5

Vulnerability Disclosure

Key Concepts
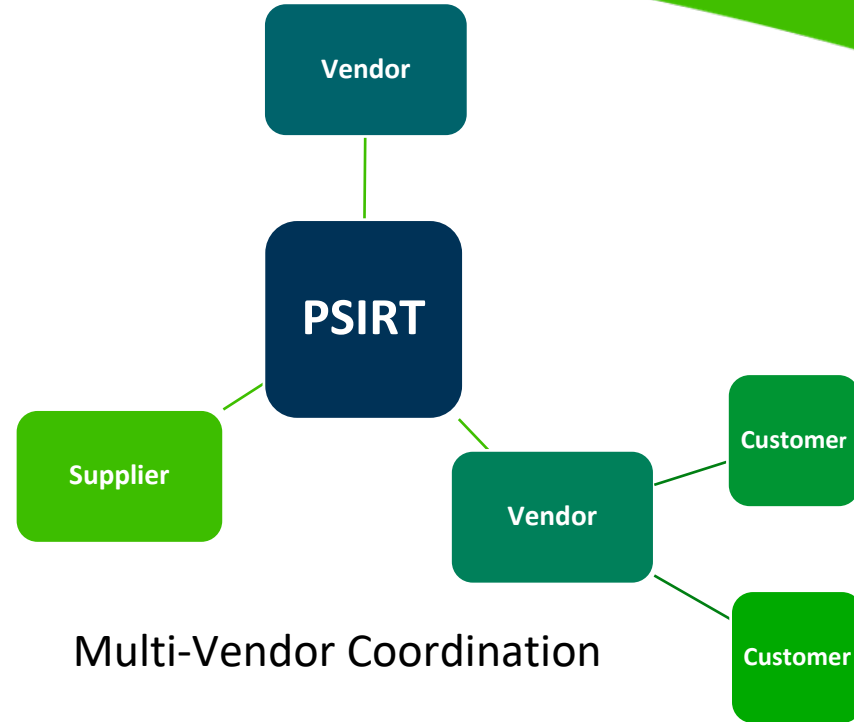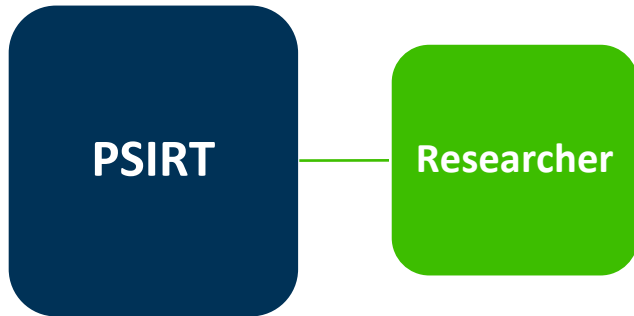
Vulnerability
Disclosure
(Service Area 5)
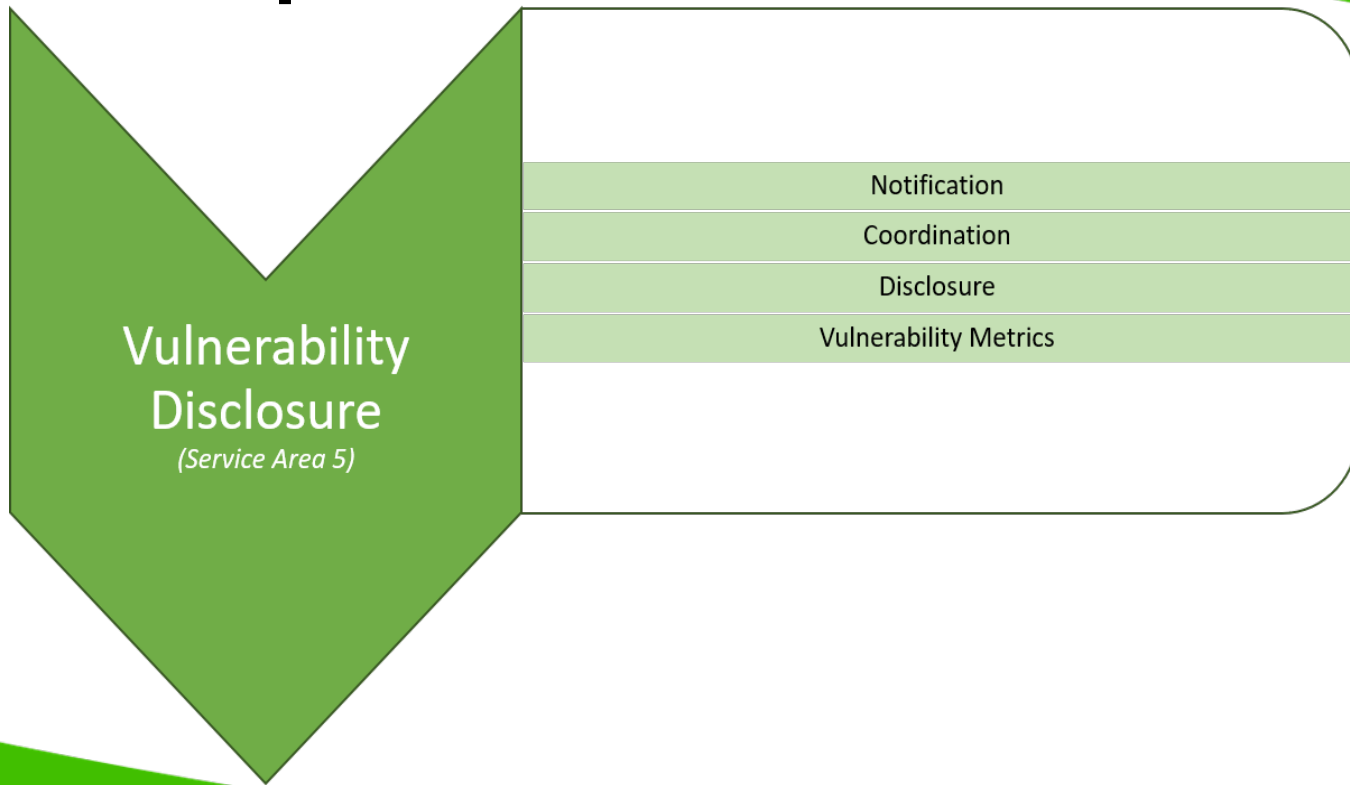
Notification

Coordination

Disclosure

Vulnerability Metrics

FIRST

Notification

Identify	• Stakeholders	
Plan	• Communication Method	Vulnerability
Coordinate	• Engage coordination center	Disclosure
Notify	• Vendors and stakeholders	Policy

FiRST
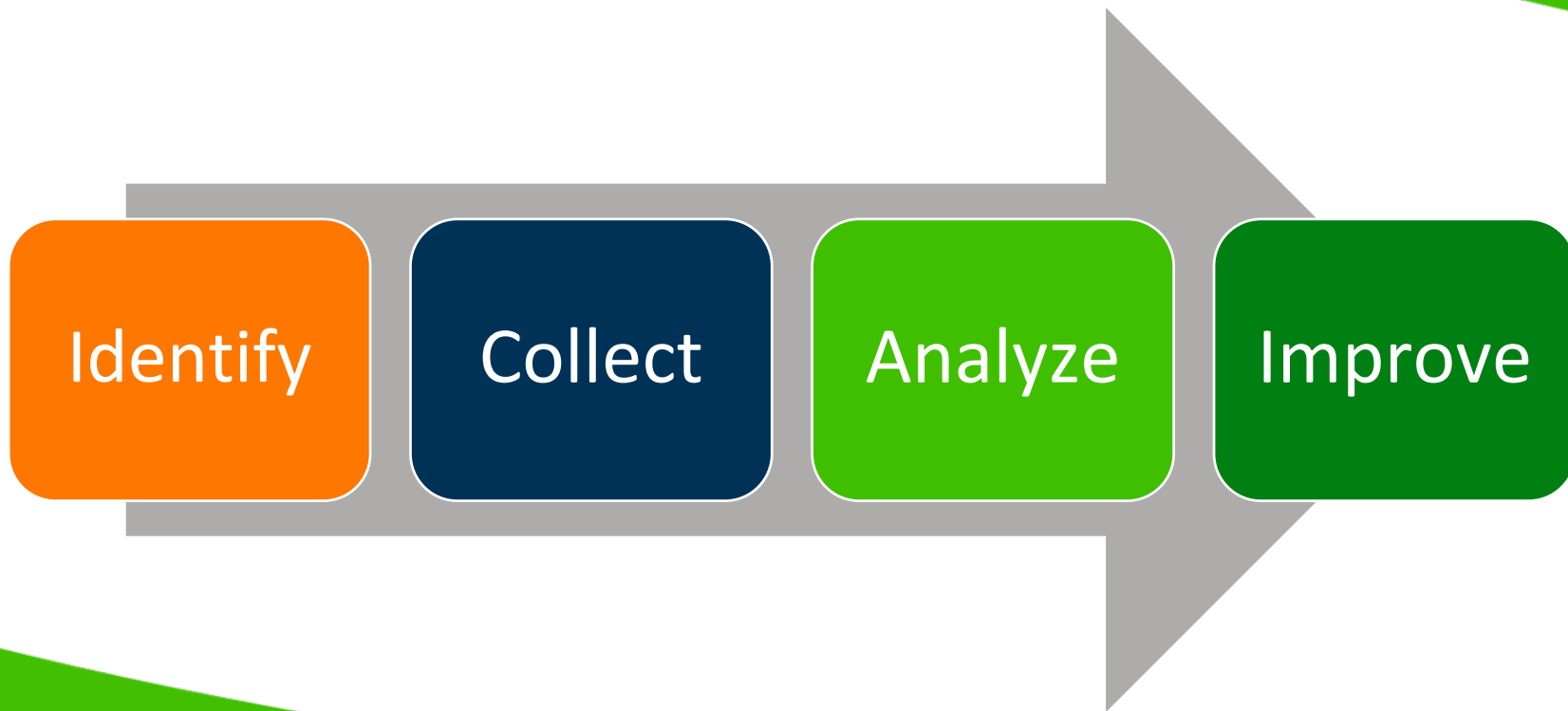
Coordination

Bilateral Coordination

Multi-Vendor Coordination

Disclosure

- Identify mechanism for disclosure
  - Release Notes
  - Security Advisories
  - Knowledge-Based Articles
  - Internal Stakeholders
- CVSS v3.0 Score
  - https://www.first.org/cvss/calculator/3.0
- CVE Assignment
  - https://cve.mitre.org/cve/cna.html

Vulnerability Metrics

Identify | Collect | Analyze | Improve

Conclusion

- Document a Vulnerability Disclosure Policy and make it available to your stakeholders

- Establish a method by which to publicly disclose security advisories and be consistent.

- Coordinated disclosures help everyone

- Use data to drive continuous improvement for your PSIRT and its supporting functions

FiRST

Copyright

Copyright © by Forum of Incident Response and Security Teams, Inc.

FIRST.Org is name under which Forum of Incident Response and Security Teams, Inc. conducts business.

This training material is licensed under Creative Commons Attribution-Non-Commercial-Share-Alike 4.0 (CC BY-NC-SA 4.0)

FIRST.Org makes no representation, express or implied, with regard to the accuracy of the information contained in this material and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

All trademarks are property of their respective owners.

Permissions beyond the scope of this license may be available at first-licensing@first.org