

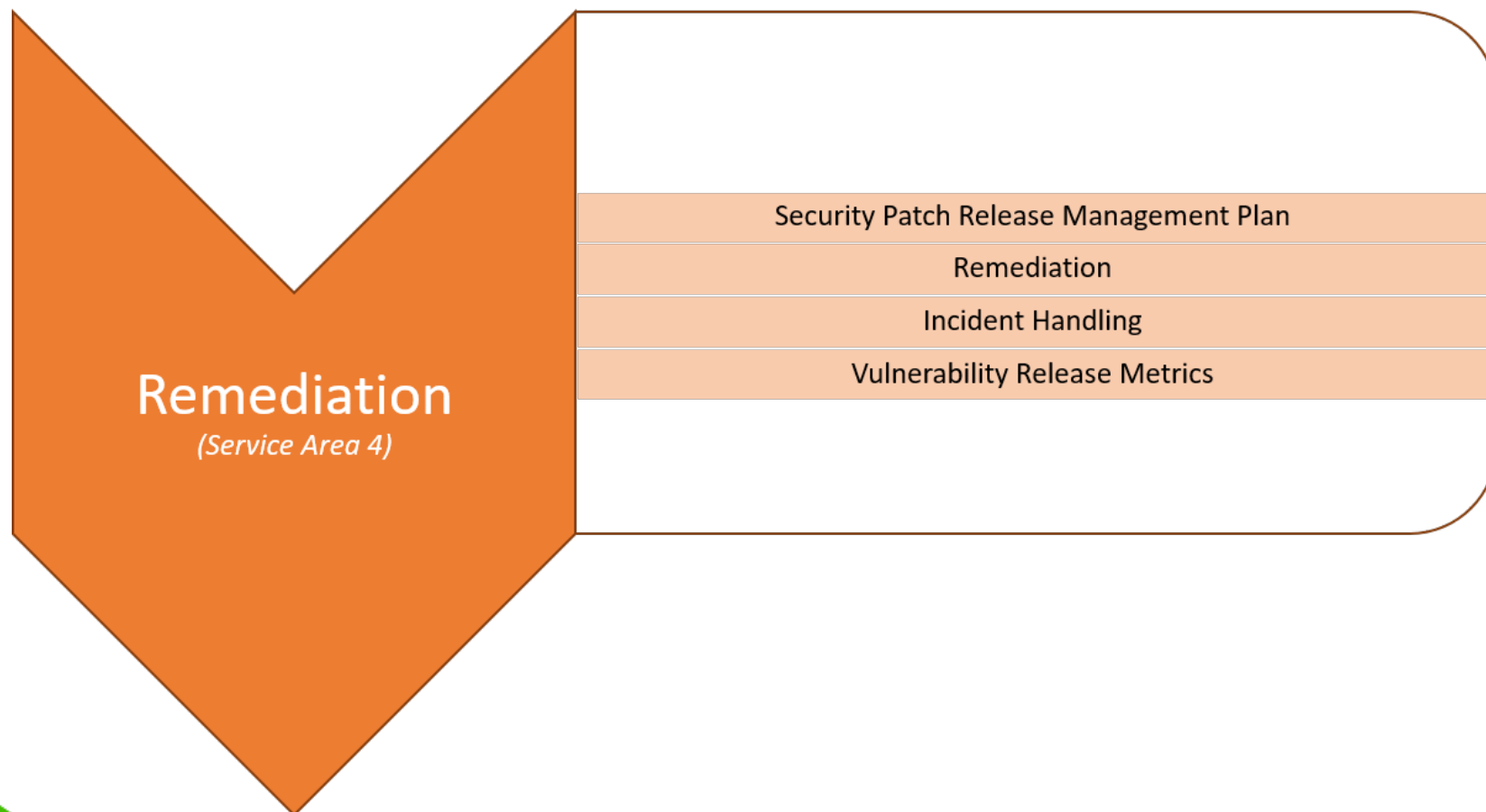
PSIRT Framework

Service Area 4

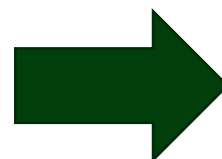
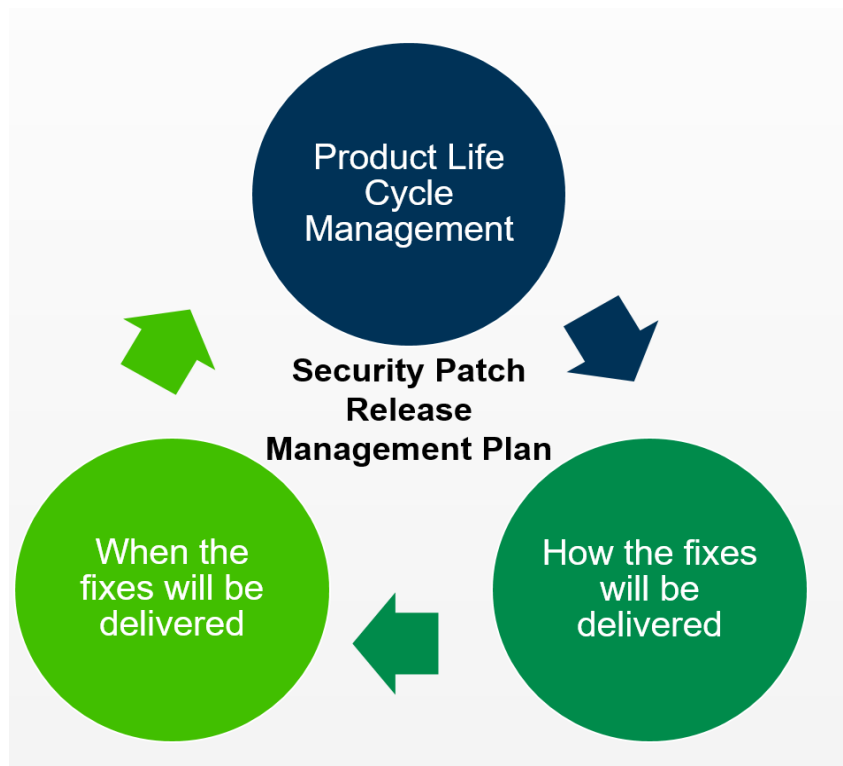
Remediation



Key Concepts



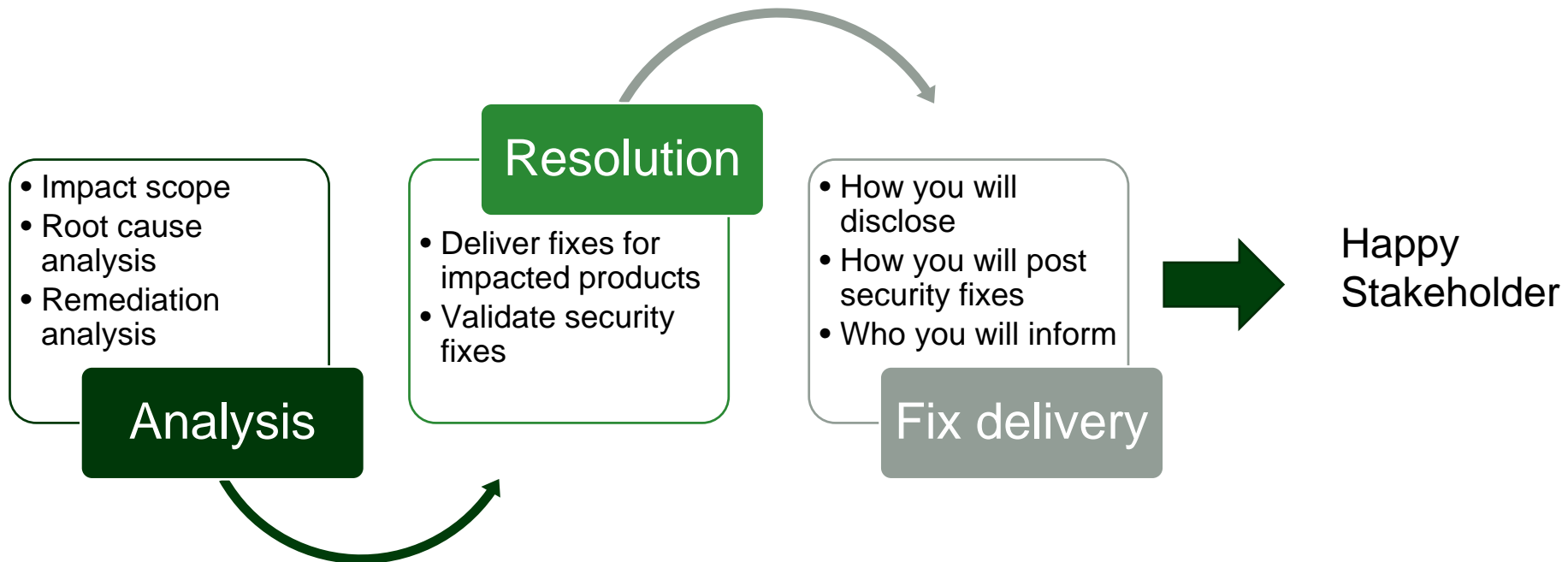
Setting the foundations for consistency



Stakeholder view

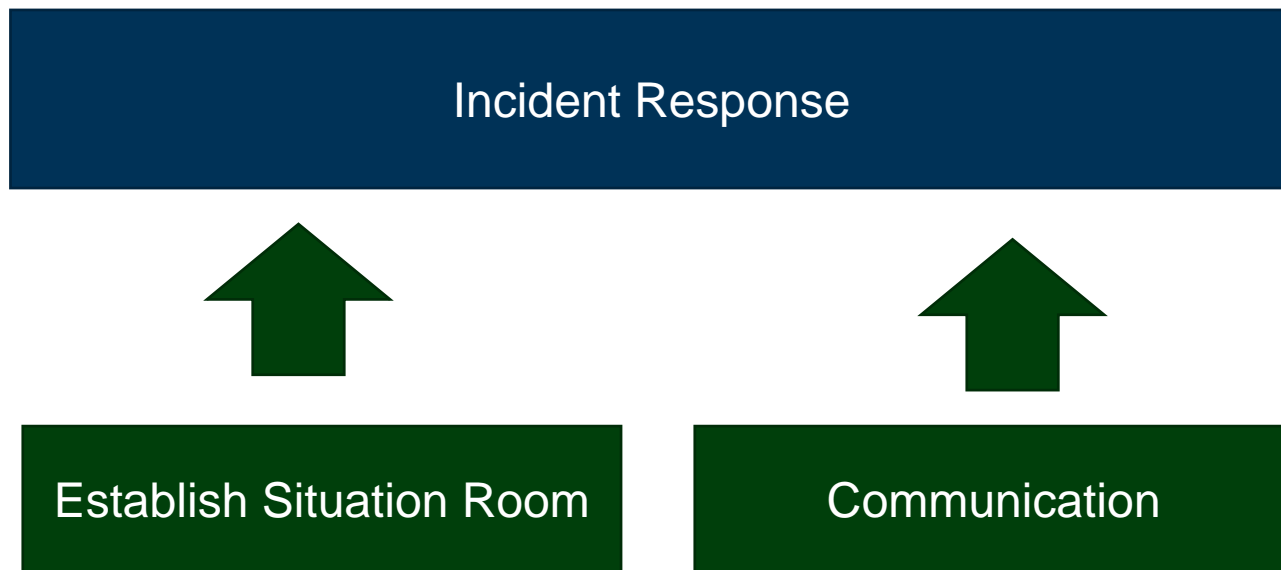
- ✓ Plan for security fixes
- ✓ Be able to easily deploy security fixes

Remediating the reported vulnerability



Risk Management Process

Alert! We have an incident



Measure. Report. Improve

Operational

- # of confirmed vulnerabilities
- # of third party components
- Categorized by CWE

Business

- On-time impact assessment and fix plan
- Remediation tracking
- On-time remediation rate



Conclusion

- Educate stakeholders on which products will be supported, mechanism and cadence for delivering security fixes.
- Establish process to analysis, remediate and validate security fixes
- Be prepared for unexpected events or emergencies
- Identify areas requiring analysis, resource, improvements by having operational and business reports



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



