PSIRT Framework

Service Area 3

Vulnerability Triage and Analysis

Key Concepts

Vulnerability
Triage and Analysis
(Service Area 3)

Vulnerability Qualification

Established Finders

Vulnerability Reproduction
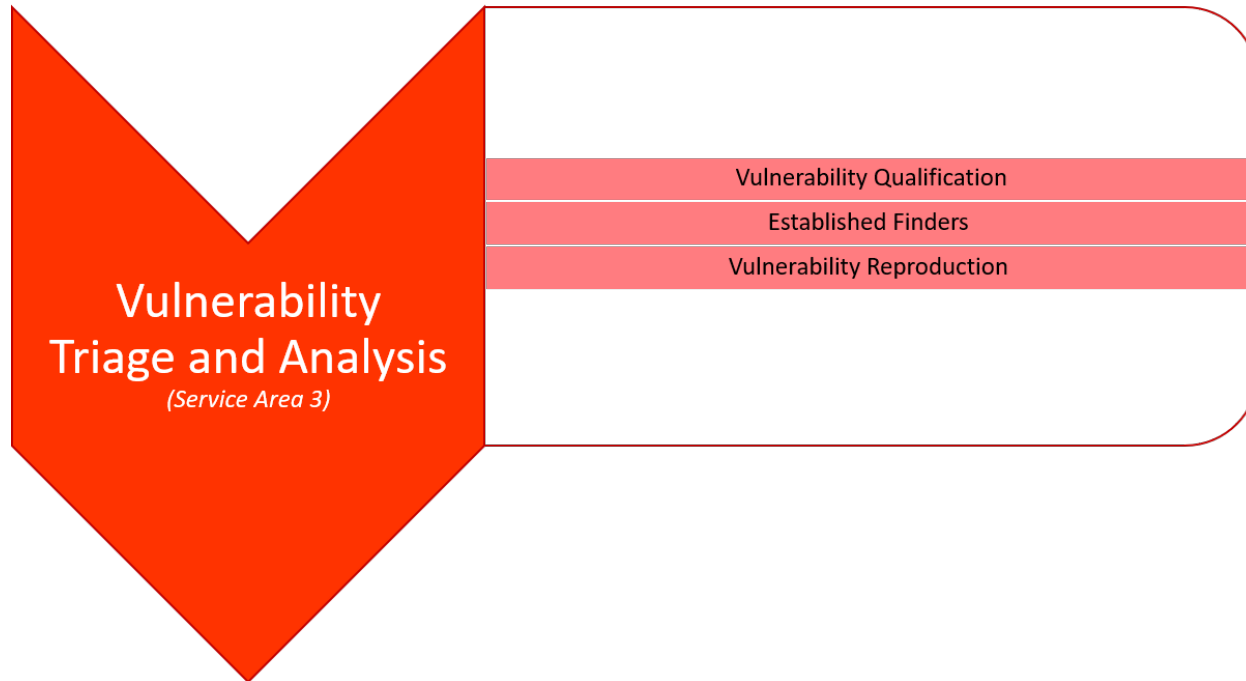
Vulnerability Qualification

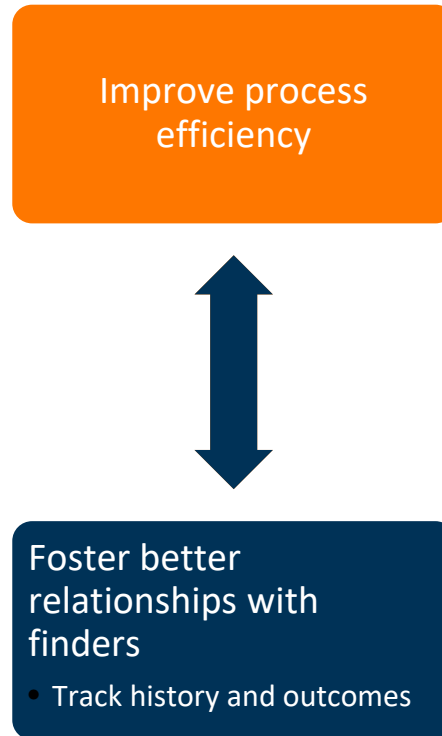Define what constitutes a vulnerability

Define how vulnerabilities are prioritized

Do this before products are released
- Document
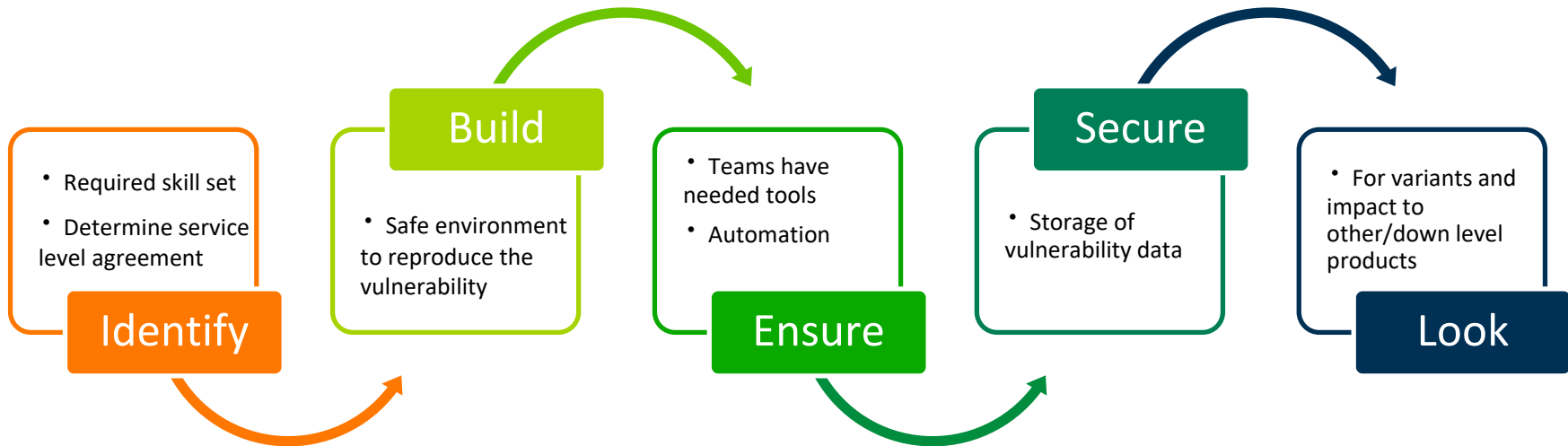- Ensure product development teams are aligned
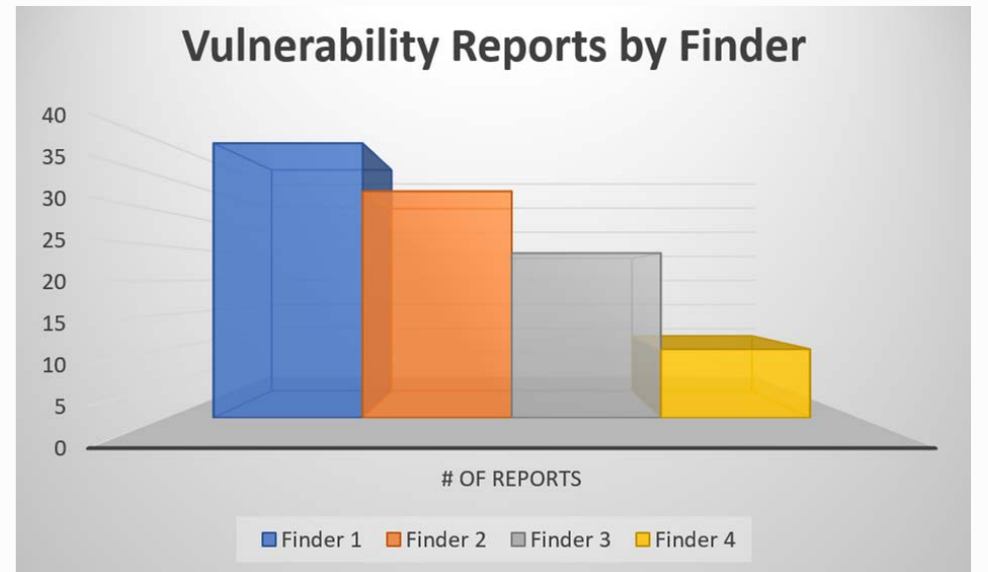
Expediting Reports from Known Finders

Improve process efficiency

Foster better relationships with finders
- Track history and outcomes

Vulnerability Verification/Reproduction

Identify
- Required skill set
- Determine service level agreement

Build
- Safe environment to reproduce the vulnerability

Ensure
- Teams have needed tools
- Automation

Secure
- Storage of vulnerability data

Look
- For variants and impact to other/down level products

Metrics

- Affected products and impact
- Variants
- Reports by finder

Vulnerability Reports by Finder

OF REPORTS

Finder 1   Finder 2   Finder 3   Finder 4

Conclusion

- Establish documented qualification processes

- Understand the security researcher community and expedite reports from known finders

- Ensure the PSIRT has the tools needed to reproduce finder reports or has agreements in place with engineering teams to do this work

Copyright