black hat®
USA 2016

Building a Product Security Incident Response Team: Learnings from the Hivemind

Kymberlee Price
Senior Director of Researcher Operations
bugcrowd

July 30 - August 4, 2016 / Mandalay Bay / Las Vegas

WHOAMI?

- Senior Director of a Red Team
- PSIRT Case Manager
- Data Analyst
- Internet Crime Investigator
- Security Evangelist
- Behavioral Psychologist
- Lawful Good

@kym_possible

AGENDA

- People
- Process
- Infrastructure and Technology
- Pitfalls
- Free Resources

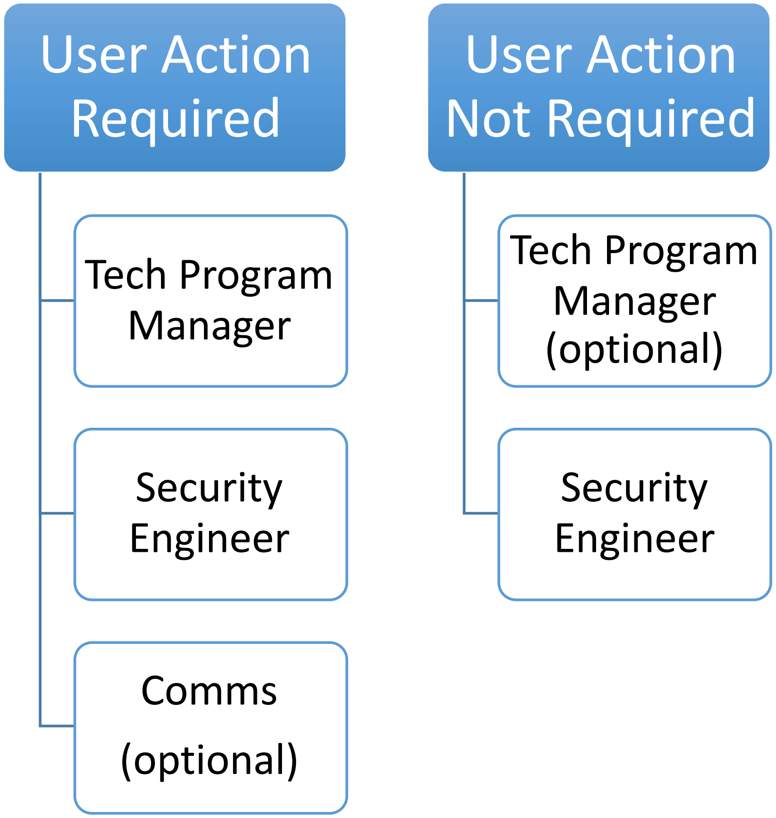
But what about ISO standards!?

- In April 2016 ISO 29147 on Vulnerability Disclosure techniques was made free to the public.
  - This is awesome
  - The related standard on vulnerability handling processes, ISO 30111 costs approx $60 USD.

PEOPLE

COMMON SIRT STRUCTURES

- Technology
  - Cloud/Service or Installed Software?
- Resources
  - $$$



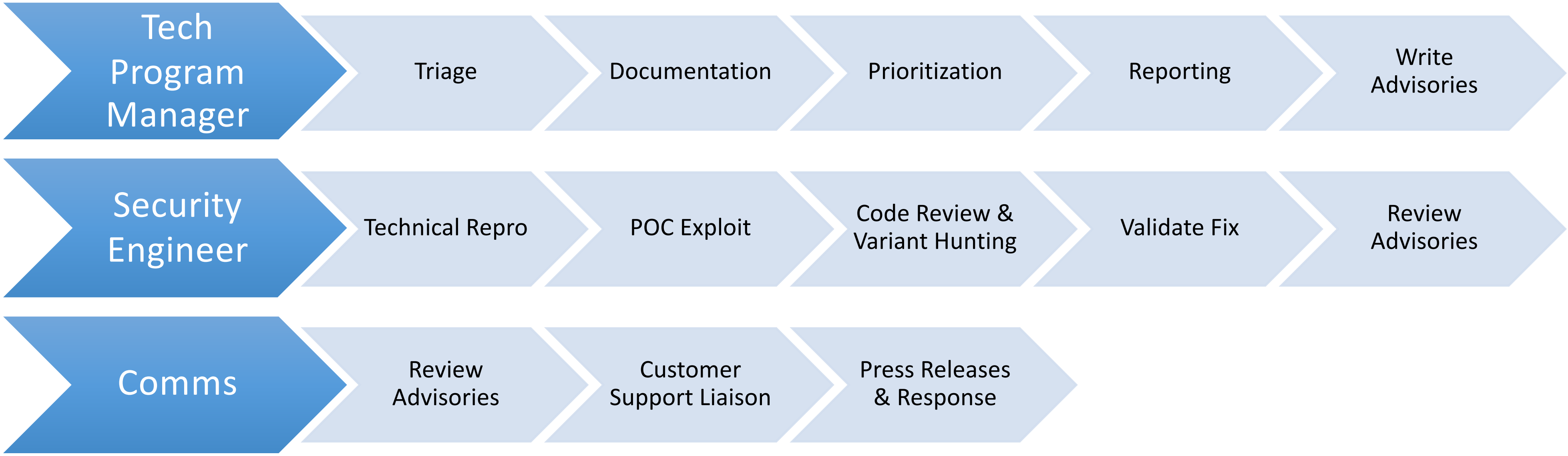
User Action Required

- Tech Program Manager
- Security Engineer
- Comms (optional)

User Action Not Required

- Tech Program Manager (optional)
- Security Engineer

TYPICAL ROLE RESPONSIBILITIES



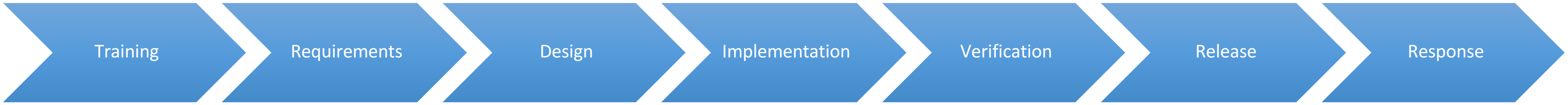
Tech Program Manager → Triage → Documentation → Prioritization → Reporting → Write Advisories

Security Engineer → Technical Repro → POC Exploit → Code Review & Variant Hunting → Validate Fix → Review Advisories

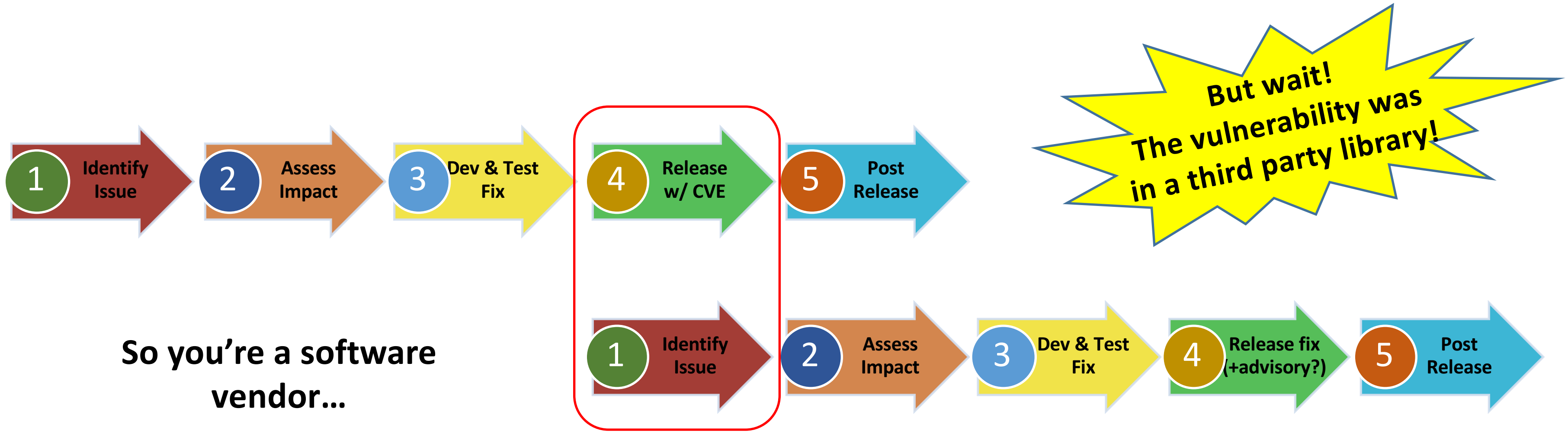
Comms → Review Advisories → Customer Support Liaison → Press Releases & Response

Process

SDL Overview



INCIDENT RESPONSE PROCESS



1 Identify Issue

2 Assess Impact

3 Dev & Test Fix

4 Release w/ CVE

5 Post Release

But wait!
The vulnerability was
in a third party library!

So you're a software vendor…

1 Identify Issue

2 Assess Impact

3 Dev & Test Fix

4 Release fix (+advisory?)

5 Post Release

INTERNAL POLICY

- Define your Vulnerability Prioritization model
  - CVSS or something else?
  - What are your acceptable business risks?
- What are your remediation SLAs? Escalation paths?
- When do you release a public advisory?
- When is emergency response indicated?

Infrastructure & Technology

Public Documentation

- Vulnerability Disclosure Policy
  - Critical for expectation setting
  - Tells researchers how to report a vulnerability to you
- Security Advisory Knowledge Base
  - Where do customers go to quickly learn about security updates
- Researcher Acknowledgements
  - Recognize positive behavior and build community

TOOLKIT

- How do you want to receive external vulnerability reports?
  - Unstructured: encrypted email
  - Structured: secure web form

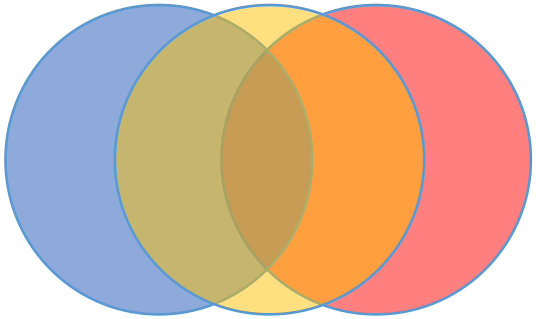
- How do you want to capture investigation details?
  - Case management db (doesn’t have to be complicated, can be specific fields captured in Jira)

TOOLKIT

- Do you use third party code?
  - Source code scanning tool to track what you use, where
  - Vulnerability Intelligence sources
  - HIGHLY RECOMMENDED: OSS SECURITY MATURITY: TIME TO PUT ON YOUR BIG BOY PANTS!
    Jake Kouns & Christine Gadsby, Jasmine Ballroom, 2:30 pm

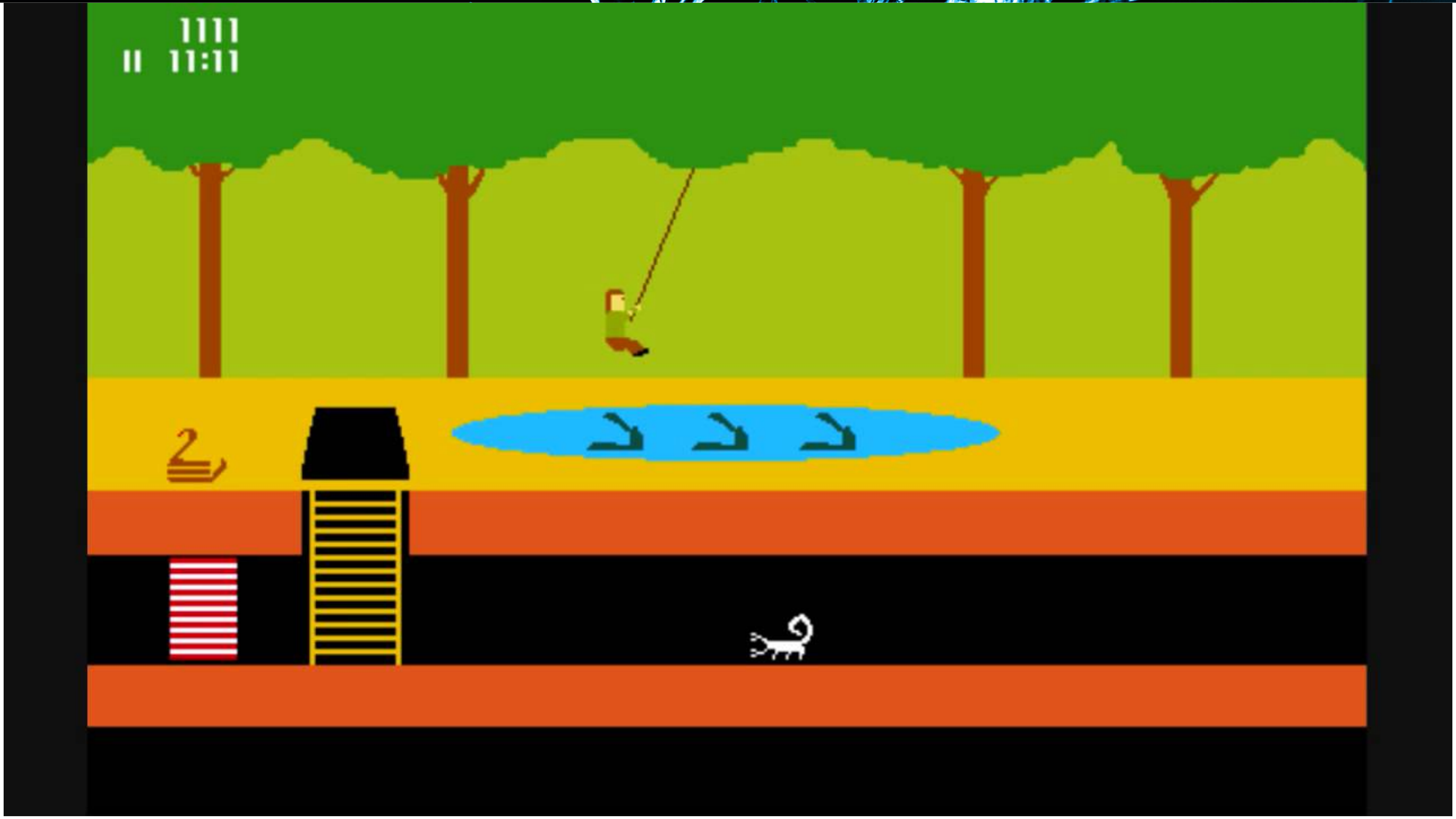
DATA MANAGEMENT FOR SIRTs

- What Developers need to know to fix vulnerability
- What Leadership needs to know about business risk
- What Customers need to know about product security



- DOCUMENT at time of investigation even if you don’t use the data until much later

Pitfalls


1111
II 11:11

PITFALLS

- Failure to thoroughly document vulnerability details during investigation, leading to re-investigation just prior to fix release to remember what the issue was
- Failure to prioritize effectively
  - Adopt a prioritization model that considers both technical and business impact
  - Define your acceptable business risks
- Failure to define clear stakeholders and roles in Incident Response Process
- Failure to communicate effectively with product development

PITFALLS

- Failure to communicate with external researchers about status of their vuln reports
  - Trust problems lead to conflict, conflict costs money
- Failure to prioritize effectively
  - Adopt a prioritization model that considers both technical and business impact
- Failure to define clear stakeholders and roles in Incident Response Process
  - Trust but verify
- Failure to communicate effectively with product development

FREE RESOURCES

- Disclosure policy basic template:
- Investigative data collection checklist
- Advisory checklist
- ISO 29147

https://pages.bugcrowd.com/best-practices-for-security-incident-response-teams

QUESTIONS

Thanks for attending!

@kym_possible

kymberlee@bugcrowd.com