Japanese Manufacturing, Killer Robots, & Effective Incident Handling

With Scott & Kevin
Introduction

- Who We Are
- What We’re About
- What We’re Gonna Share
Who We Are?

Kevin aka @bfist
Response Lead @ Heroku

Scott aka @sroberts
SIRT Lead @ GitHub
FOR578 Instructor
WHAT WE’RE ABOUT?

MAKING INCIDENT RESPONSE MORE EFFICIENT WITH SCIENCE ENGINEERING
WHAT WE’RE GONNA SHARE?

A LOW COST, COLLABORATIVE METHOD FOR MANAGING COMMON INCIDENT RESPONSE WORKFLOWS
You’ve Got 99 Problems

- Moving up the Maturity Model
- Enable multiple responders
- Provide easy to comms to stakeholders
- Incidents come in waves
- You’re poor and have no $$$
Characteristics of the Maturity levels

- **Level 1: Initial**
  - Processes unpredictable, poorly controlled and reactive

- **Level 2: Managed**
  - Processes characterized for projects and is often reactive.

- **Level 3: Defined**
  - Processes characterized for the organization and is proactive.
    - Projects tailor their processes from organization's standards

- **Level 4: Quantitatively Managed**
  - Processes measured and controlled

- **Level 5: Optimizing**
  - Focus on process improvement

*Project Management*
JIT
(Just In Time)

- Management Theory from Toyota
- Create as Needed/Not as Planned
- Limits Inventory
- Lots of IR Parallels
Introduction to Kanban

- A factory floor level production management tool
- Spatial representation of tasks through a series of phases
- Adapted to multiple non-manufacturing industries
Introduction to Kanban
<table>
<thead>
<tr>
<th>Stories</th>
<th>To Do</th>
<th>In Progress</th>
<th>Testing</th>
<th>Done!</th>
</tr>
</thead>
<tbody>
<tr>
<td>US No: 10</td>
<td>US No: 8</td>
<td>US No: 7</td>
<td>US No: 5</td>
<td>US No: 1</td>
</tr>
</tbody>
</table>

Thumbs up!
Useful For...

- Short Term (JIT) Tasks Around Incidents
- Long Term Management Task for Projects & Continuous Output
Warning

We use the same tool (Kanban)  
BUT…

We use kanban very differently  
(And that’s cool!!!)
### Example Response

#### All Incidents

<table>
<thead>
<tr>
<th>Task</th>
<th>Added by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create incident record</td>
<td>blackfist</td>
</tr>
<tr>
<td>Perform initial triage</td>
<td>blackfist</td>
</tr>
<tr>
<td>Create timeline document</td>
<td>blackfist</td>
</tr>
<tr>
<td>Notify management (level 2 or higher)</td>
<td>blackfist</td>
</tr>
</tbody>
</table>
Platforms: GitHub Projects

- Notes, artifacts, and boards in one place
- Assign cards to people
- Easy API
- No Built In Templating
GitHub Projects

- Backlog 3
  - Flip the switch
    - #10 opened by nakajima
  - Spread the word on Twitter
    - Added by katelynbryant
  - Add and update documentation for new features
    - Added by jeaver

- Ready 1
  - Design project graphic
    - #9 opened by mdo

- In progress 2
  - Draft blog post
    - #7 opened by stephbwillis
  - Perform security audit
    - #8 opened by DarcyCK
Platforms:

- Trello

- Kanban is their main product
- Full featured GUI
- Card based discussions
- Attachable Files
- Many Integrations
- Mature API
Trello
Incident Stages

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

} Built Here

Helps Here
- Build template Kanban boards for common incidents
- Start with a column for basic information sharing
- Do you have things that need to be done in every incident?
Other Stages

- Create a column for containment, eradication, and recovery tasks.
- Do you need to roll creds for this incident?
- Do you need to revoke hardware tokens?
Example: Malware Incident
Lessons Learned

- Create a column for lessons learned
- Dumping ground for the retro
Meat & Potatoes (And Simplicity)

- 3 Columns
- In Progress
- Done
- Canceled
- Assign People to Tasks
- Canceled cards should have an explanation
Example

In Progress
- Attach/detach shogun/yobuko databases to transfer
- engage legal for messaging

Done
- Prepare to notify CSIRT of the incident
  - Create a chat room channel for the incident
    - Start a document to track details

Cancelled
- If anyone involved needs time off for personal recovery, suggest scheduling some
  - Add a card...
Example: Lost/Stolen Laptop

**Basic information**
- Links to detailed notes
- Case points of contact

**Containment**
- Create incident record
- Verify disk encryption
- Revoke user’s Yubikey
- File police report
- (optional) Cred Rolls

**Lessons Learned**
- (optional) Schedule a retrospective

**In progress**
0

**done**
0
Workflows:
System Triage

- New
- Live Response Requested
- Live Response Received
- Analyzed
- Remediated
- Returned
Workflows:
Compromised Resources

- Malicious Activity Identified
- Password Reset
- 2FA Verified
- User Interviewed
- Remediated
Workflows:

Indicator Development

- Backlog
- Enriched
- COA: Discovery
- Detection Created
- COA: Detection Deployed
- Detection Deprecated
Workflows:
- Planned
- Analyzed
- Drafted
- Edited
- Released
- Feedback Collected
- Templates move you from managed to defined
- Repeatable & Consistent
- Demonstrate Process
- Reduce Admin Overhead
Wanna Try It?

github.com/sroberts/incident-template
Bonus Content: The Five Whys

- More Toyota Stuff
- Root Cause Analysis Methodology
- Useful Retrospective Technique
Conclusion

- Kanban helps make repeatable yet flexible processes
- Makes communications consistent
- Powerful with a little automation
Thanks

Made with <3
By Scott (@sroberts) & Kevin (@bfist)