

Playing in the Rain: Preparing for Incidents with Game Days

Kenn Hussey, ConFoo 2022

Kenn Hussey
Director of Operations
kenn@datawire.io



Agenda

01

Why?

Operational
Excellence

02

How?

Game Day
Playbook



03

WIIFM?

Lessons
Learned



Why?

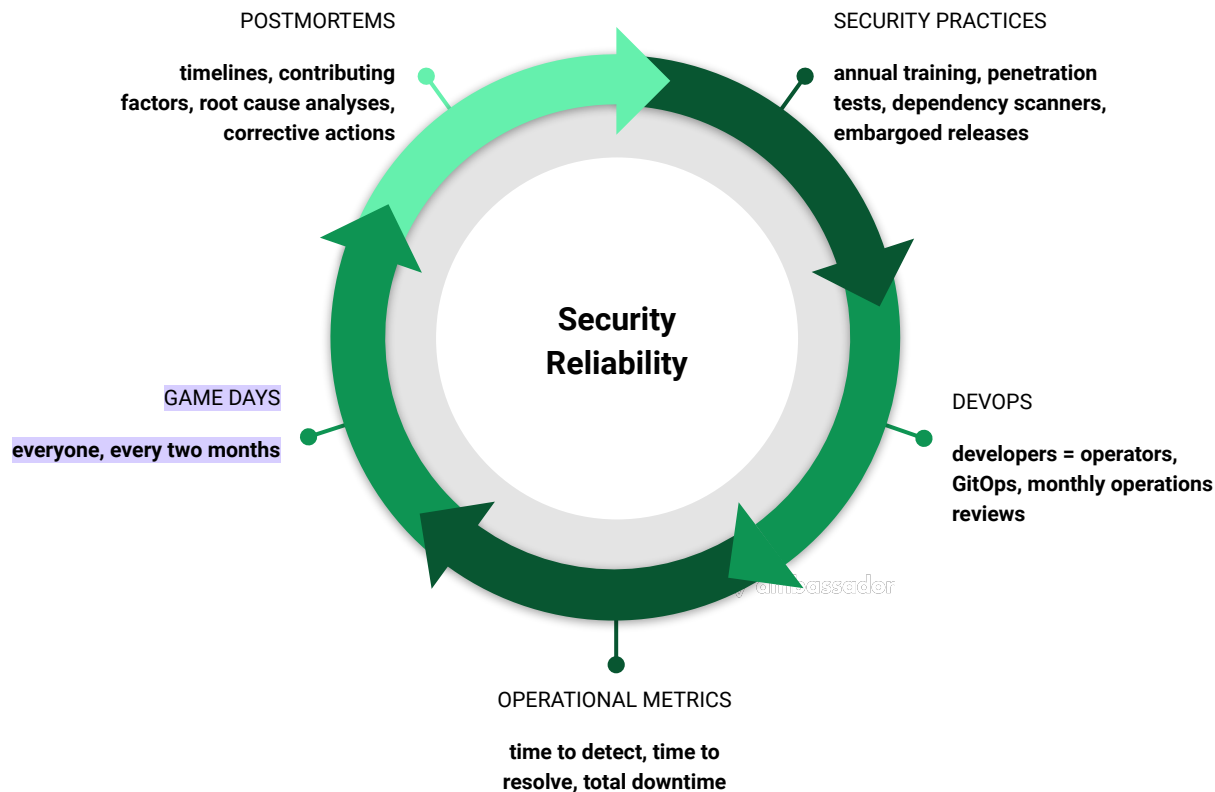
Operational Excellence

Operational Excellence

- At Ambassador Labs, it's everyone's responsibility
- Our customers count on us to deliver products and services that are **secure** and **reliable**
- We work to *continuously improve* security and reliability but must be prepared to *respond effectively* in the case of an incident



Continuous Improvement



Effective Response

DECLARE

RESOLVE

DETECT



CONTAIN

INVESTIGATE

REMEDiate



RECOVER

System uptime checks

24x7 after hours phone

Alerts

- PagerDuty
- Slack
- email

On-call rotations

- Support
- Engineer
- Escalation Manager

Incident Checklists

Redundancy

Response Team

- First Responder
- Incident Commander
- Support Lead
- Engineering Lead
- Subject Matter Experts



Remediation Plan

Hotfixes

ChatOps

Patch Releases

Postmortems

Corrective Actions

Game Days

What?

Controlled exercises
(once every 8 weeks)
that simulate real
incidents to practice our
ability to respond to
them

Who?

Everyone, but focused
on anyone that's on call
(Engineering, Support,
Management)

Why?

Improve our
processes, test system
resiliency, validate
observability
mechanisms, and
reduce stress during
real incidents



How?

Game Day Playbook

Let's Play a Game...

01

Nominate a
Game Master

02

Send out a
primer

03

Let it *rain!*

04

Use a
dedicated
Slack channel

05

Hold a
 ambassador
postmortem

06

Debrief with
the team

Roles and Responsibilities

Game Master

Takes care of triggering the incident, keeps notes and monitors the game in case it needs to be aborted, and holds a debrief to review key takeaways

Accomplices

Assist the Game Master with carrying out the exercise (e.g., by pretending to report an anomaly)

Responders

On call staff and Subject Matter Experts that investigate and resolve the incident

Planning the What

scenario

What scenario will be tested by this exercise?

target

What product(s) and/or or service(s) will be targeted?

hypothesis

What is your hypothesis for how the scenario will play out?

takeaways

What do you expect to be the key takeaways from the exercise?

cost

What impact(s) will the exercise have on the business?



Planning the Who

stakeholders Who will be affected by the exercise?

accomplices Who will be involved in conducting the exercise?

responders Who do you anticipate will respond to the incident?

SMEs Who are the Subject Matter Experts for the target products/services?

reviewers Who should review the plan for awareness and/or approval?



Planning the When

start

When will the exercise start?

end

When will the exercise end and under what circumstances will it end early?

debrief

When will the debrief be (be sure to allow time for a postmortem)?



Planning the How

trigger

How will the incident be triggered?

resolution

How should it be resolved?

nudge

How will responders be “nudged” if they don’t respond as expected?

halt

How will the exercise be halted if it needs to end early?



One Rainy Day at Ambassador Labs...

scenario Introduce a typo in one of the shortened web links used by Marketing.

target Business critical links that are managed in Bit.ly.

hypothesis We won't notice the problem and will struggle to fix it once prompted.

takeaways No monitoring in place, incomplete and redundant documentation.

cost Potential users won't be able to follow the link during the exercise.





WIIFM?

Lessons Learned



Improvements to Date



Better
procedures for
responding to
customer
outages



Increased clarity
around incident
roles and
responsibilities



Improved
alerting for
system uptime
checks



Streamlined
reporting of
customer
incidents



Faster response
times for
business hours
outages

Best Good Practices



Rotate the Game Master responsibility so everyone gets a turn



Make scenarios as realistic as possible - rain, not sun!



Actually follow through on corrective actions



Schedule them when it's less disruptive and stressful for the team... or not!



Crawl before you walk... and then run!

Thanks!

We're Hiring!

<https://www.getambassador.io/about-us/careers/>

kenn@datawire.io