Upside Down: Crisis Management Automation

Swathi Joshi
Senior Technical Program Manager- Response

Us

Swathi Joshi
Senior Technical Program Manager
sjoshi@netflix.com

Members of the Security Incident Response Team (SIRT)

Overview

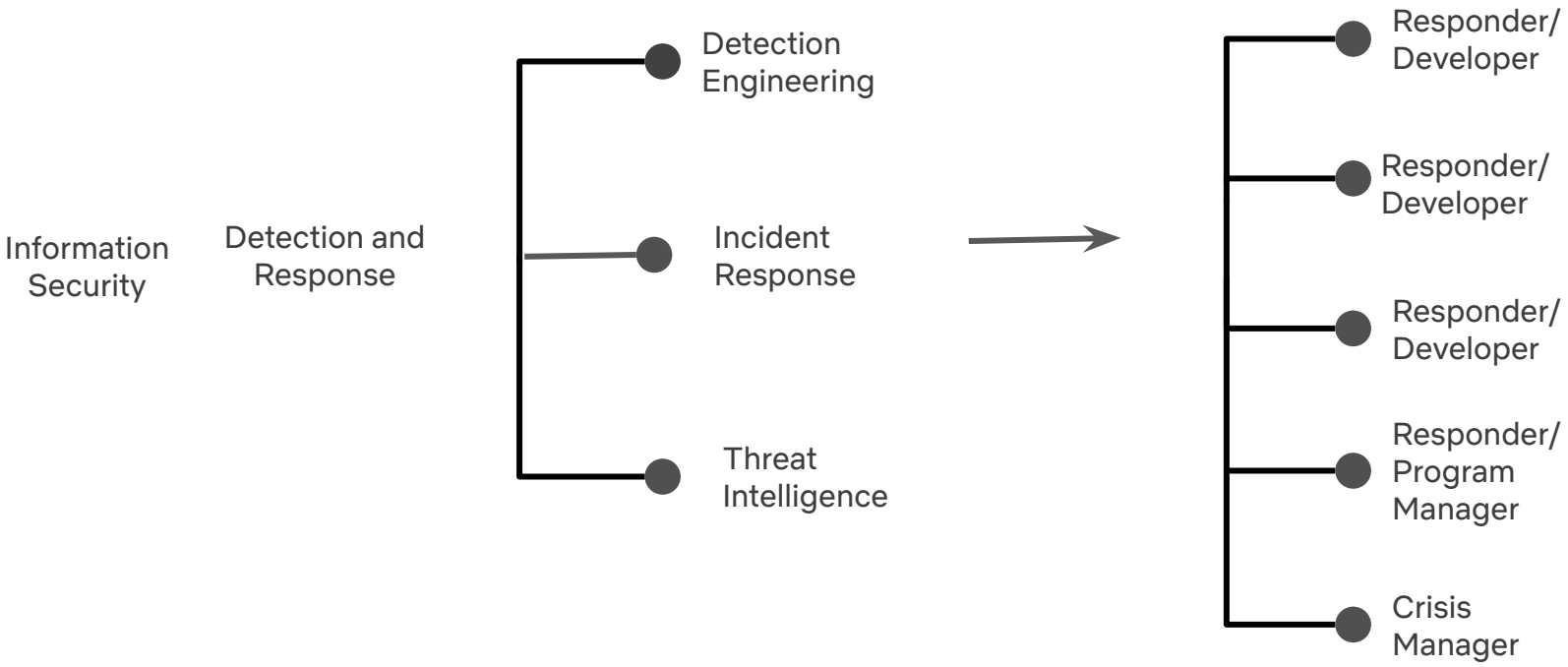
- What?
  - Culture of IR
- Why?
- How?
  - Incident Lifecycle
- Impact
  - Roadmap

NETFLIX

What?

Problem are we trying to solve

Team Structure



NETFLIX

Incident Response Mission

We strive to detect quickly, respond effectively, and limit blast radius from security events vs. prevent every incident

Culture of Incident Response

- Incident Vs. Crisis
- Fix Vs. Prevent
- Context Vs. Control
- Good Vs. Bad Process
- SOC Vs. SOC-less

NETFLIX

Enabling Pillars

Training
Incident Lead and Incident Participation

Tabletops
Cross Functional Simulation Exercises

Guidelines
Incident Severity, Crisis Communications

Tooling
<<more>>

Why?

are we solving it

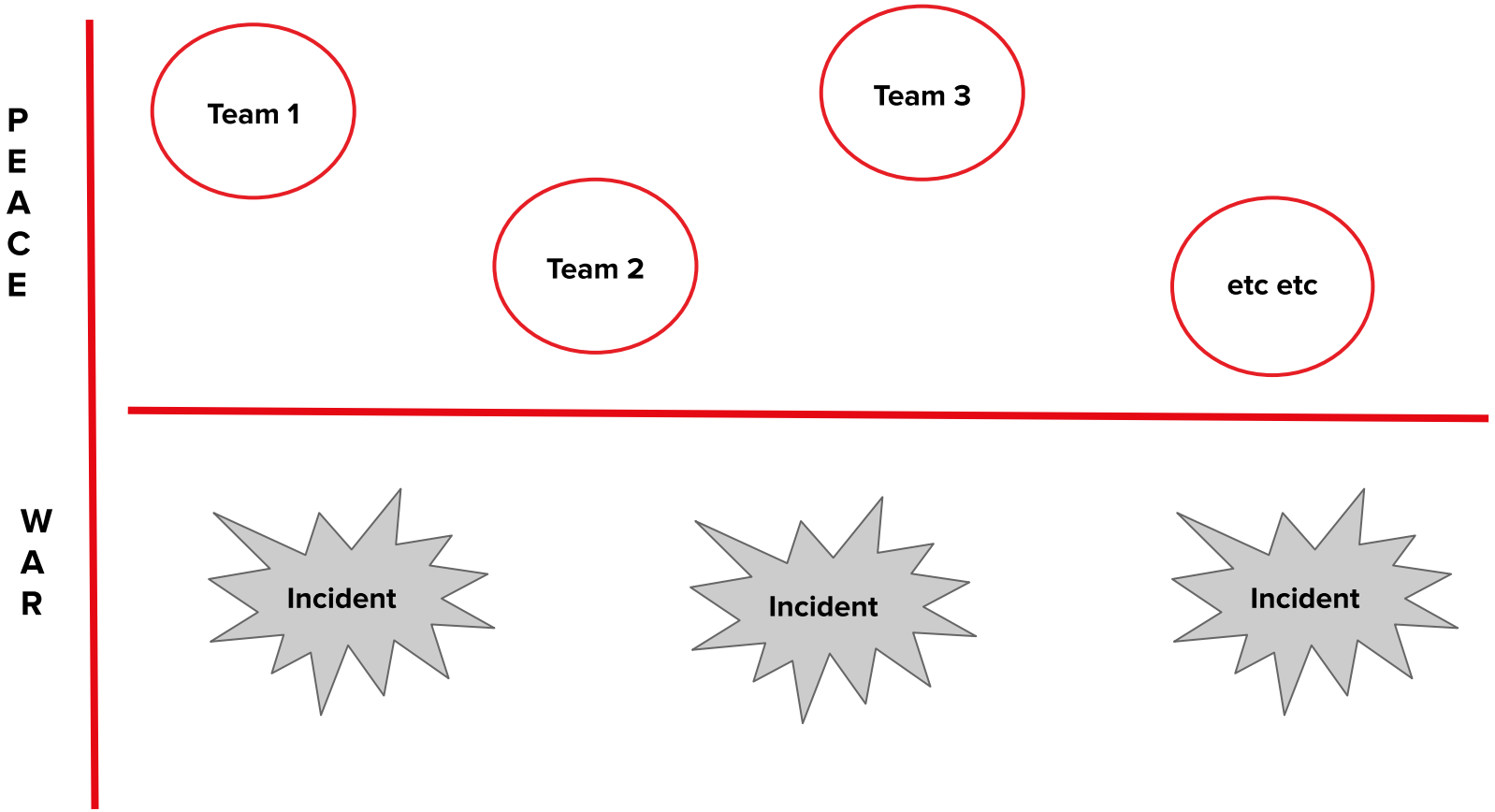
Our Story.

Distributed Model

Efficiency Mindset

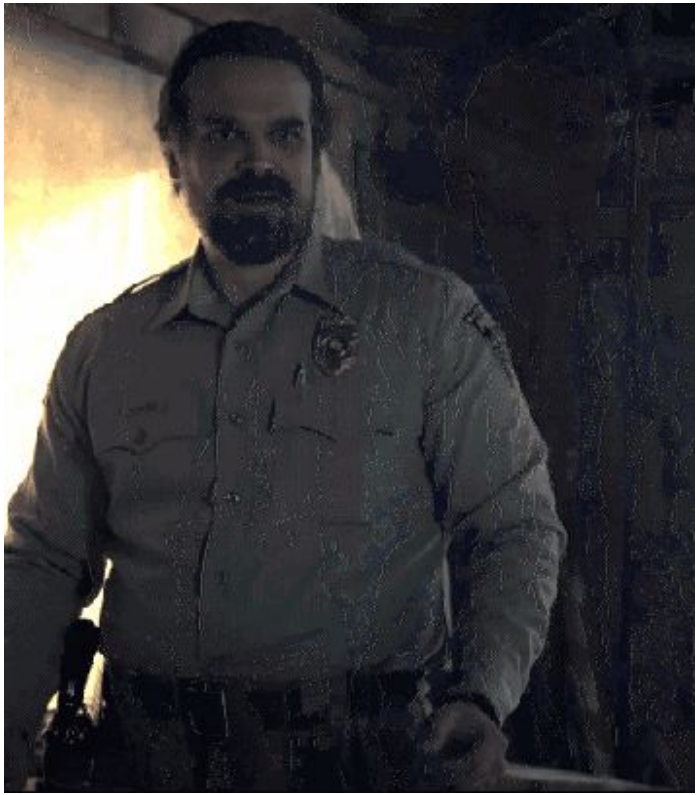
Scale

Scale


PEACE
WAR
Team 1
Team 2
Team 3
etc etc
Incident
Incident
Incident

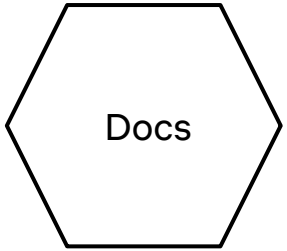
Guidelines

- Incident Severity
- Crisis Communications
- When to escalate to SIRT?
- Hand off Document
- Gameday Toolkit
- Incident Response Plan



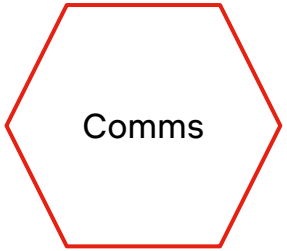
NETFLIX

~~Copy paste~~



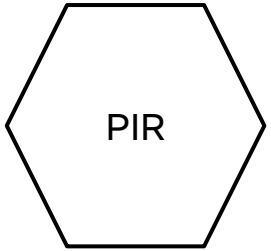
Investigation doc

Incident drive



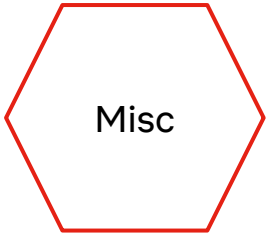
Executive update

CAN Report



Post Incident Review doc

Timeline



PIR meeting invite

Welcome Message

NETFLIX

Art of little things

- Decision Making
- Consistency
- Templates
- Mean time to Resolve
- Need help quickly

- Communication Channels
- Expectations
- Documents
- Mean Time To Assemble
- Clear expectations

NETFLIX

How?

are we solving it

Requirements Analysis

- Start wide and Go deep
- Technology agnostic
- Started with 5 pages and grew to 15 pages
- Add lightweight status

NETFLIX

Decision Log

Option 1 - Create new workflow engine

Option 2 - Buy SOAR solution

Option 3 - Leverage internal tools

Option 4 - Continue with scripting

Option 5- DO NOTHING

NETFLIX

Priority

People Resolve Incidents.

- Who do I contact? How do I contact them?
- What is this new message, can ignore it? Should I pull the car over?
- Why am I here? What do you need me to do?

Incident Ramp.

- Getting people engaged and oriented
- Leverage existing knowledge and workflows

Tech.

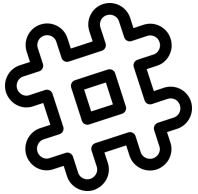
Piecing it all together.

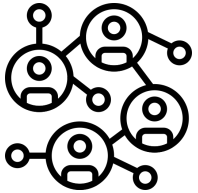
Slack and Email

Google Docs

Demisto

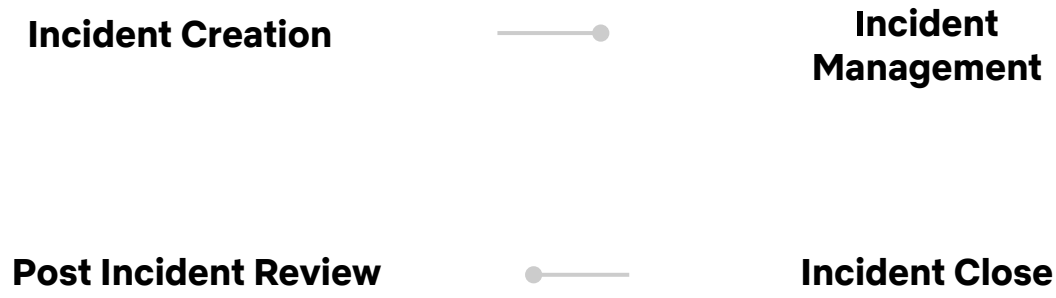
+ Many More





Walkthrough

Incident Lifecycle



Incident Creation

Step 1: Create Incident- go/securityincident fill out a form

- Create a JIRA ticket
- Creates investigation doc
- Create a incident slack channel
- Creates incident drive
- Creates two google groups
- Pulls on call and assigns it
- Includes people based on severity
- Send welcome message

NETFLIX

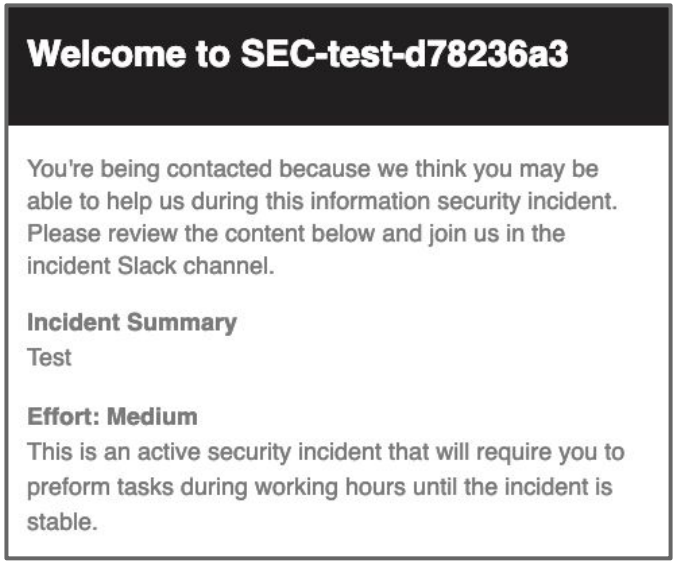
Hi.

SIRT Bot

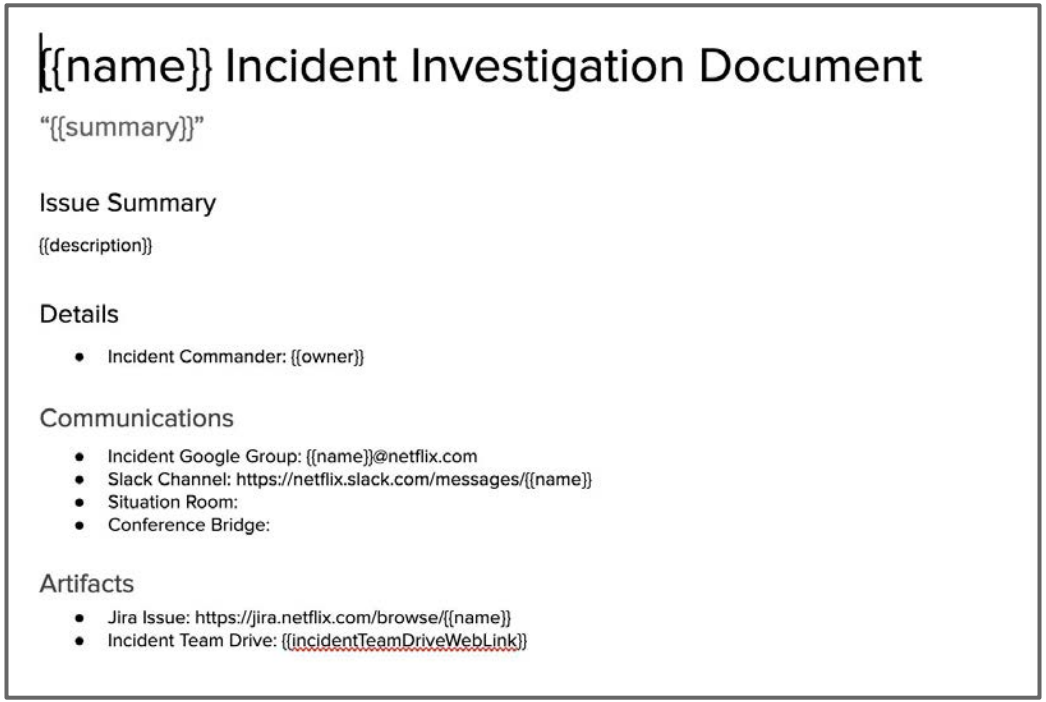
Welcome to SEC-test-d78236a3
You're being contacted because we think you may be able to help us during this information security incident. Please review the content below and join us in the incident Slack channel.

Incident Summary
Test

Effort: Medium
This is an active security incident that will require you to preform tasks during working hours until the incident is stable.



Enter text here.



{{name}} Incident Investigation Document

"{{summary}}"

Issue Summary

{{description}}

Details

- Incident Commander: {{owner}}

Communications

- Incident Google Group: {{name}}@netflix.com
- Slack Channel: https://netflix.slack.com/messages/{{name}}
- Situation Room:
- Conference Bridge:

Artifacts

- Jira Issue: https://jira.netflix.com/browse/{{name}}
- Incident Team Drive: {{incidentTeamDriveWebLink}}

Incident Management

Step 2: During an incident, we should support following capabilities

- Create physical war room invite and send to the group
- Send CAN report
- Create and send executive update
- Be able to create a timeline
- Loop in the right folks

NETFLIX

Incident Close

Step 3: After an incident closes we should

- Update associated JIRA
- Close and archive slack channel
- Create post incident review doc
- Send the feedback form

NETFLIX

Roadmap

What are we doing next?

Next Steps

Post Incident
Action Tracking

Notifications

Metrics

Dashboard
Tags- Studio- PII?
Seasonality?

Sweat the details

- Expose commands in slack
- Create incidents based on any inbound
- Onboard partner teams
- Tasks and Reminder during incident handling
- Incident hand off and refinement

NETFLIX

Thank you

NETFLIX