

# RSA<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

SESSION ID: CXO-T07

## Building Security In – DevSecOps
































































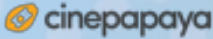














**Noopur Davis**

SVP, Chief Product and Information  
Security Officer, Comcast  
[@noopurdavis](#)



#RSAC

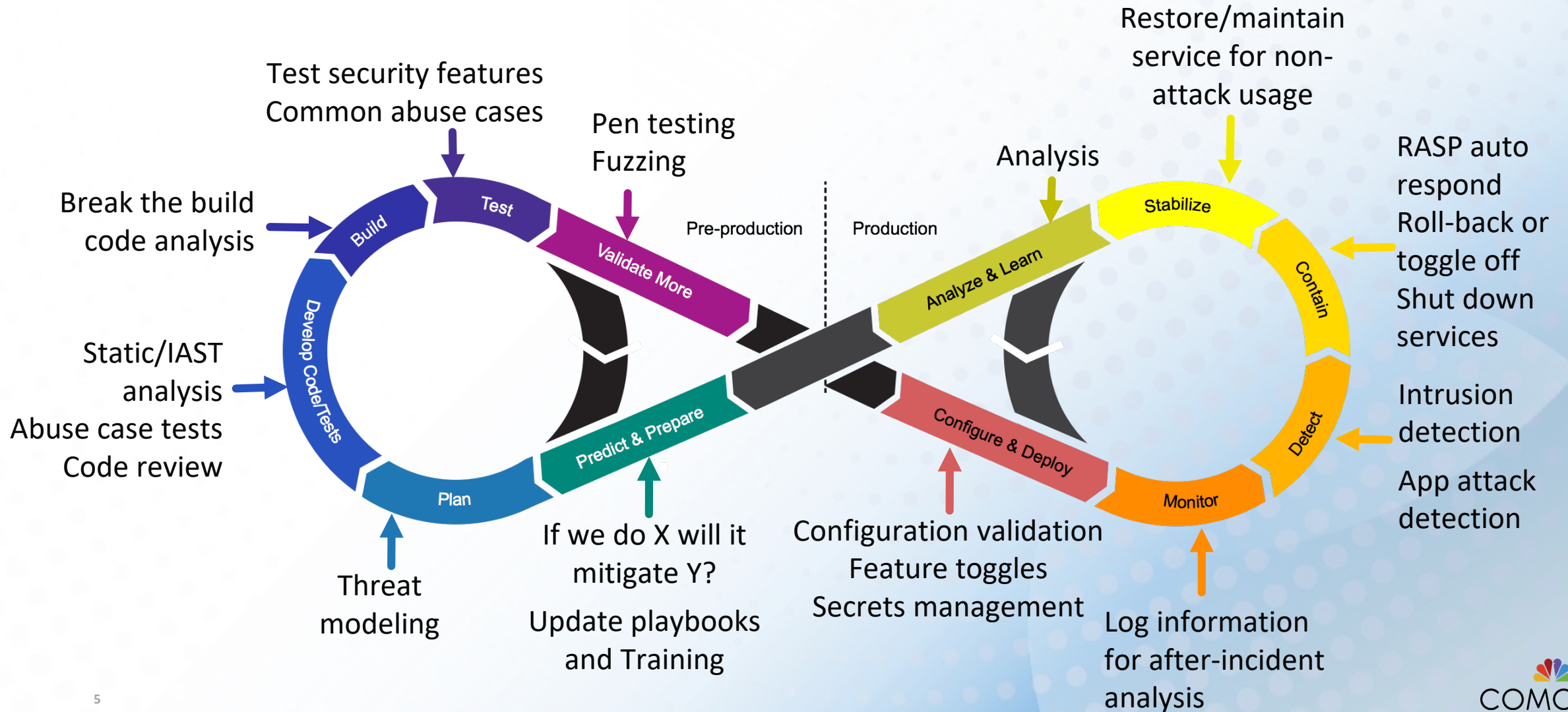
A global media and technology company with several businesses, including Comcast, NBCUniversal, and Sky.

COMCAST	NBCUniversal					sky
Products & Services	Cable Networks	Broadcast	Local Media	Film	Parks	Products & Services
<div><div></div><div></div><div></div><div></div></div>	<div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div> <div></div>	<div></div> <div></div> <div></div>
Comcast Spectacor						Channels & Content
<div></div> <div></div> <div></div>						<div></div> <div></div> <div></div> <div></div>
Partner Companies						
<div></div>						
Other						
<div></div>						
Digital & Other						
<div><div></div><div></div></div>						
<div><div></div><div></div></div>						



**DEV[SEC]OPS IS...  
EMPOWERED ENGINEERING TEAMS  
TAKING OWNERSHIP  
OF HOW THEIR PRODUCT  
PERFORMS IN PRODUCTION  
[INCLUDING SECURITY]**

# SECURITY PRACTICES ON DEVOPS CONTINUUM → DEVSECOPS



**THAT'S A LOT OF STUFF!**

**HOW DO WE GET  
DEVELOPMENT TEAMS TO  
ADOPT?**



# **A FRAMEWORK FOR DEVSECOPS**

**DEFINE PRINCIPLES**

**GET EXECUTIVE SPONSORSHIP**

**DEFINE A SECURE DEVELOPMENT LIFECYCLE**

**DEFINE A SECURITY MATURITY MODEL**

**BUILD COMMUNITY**

**PROVIDE SUPPORT**

**SUPPORT SECURITY CRAFTSMANSHIP**

# COMCAST SDL GUIDING PRINCIPLES

**BUILD SECURITY IN**  
**MORE THAN BOLT IT ON**

**RELY ON EMPOWERED ENGINEERING TEAMS**  
**MORE THAN SECURITY SPECIALISTS**

**IMPLEMENT FEATURES SECURELY**  
**MORE THAN SECURITY FEATURES**

**RELY ON CONTINUOUS LEARNING**  
**MORE THAN END-OF-PHASE GATES**

**BUILD ON CULTURE CHANGE**  
**MORE THAN POLICY ENFORCEMENT**



# SDL PROGRAM ENGAGEMENT MODEL

## ONBOARDING



## ONGOING (QUARTERLY)

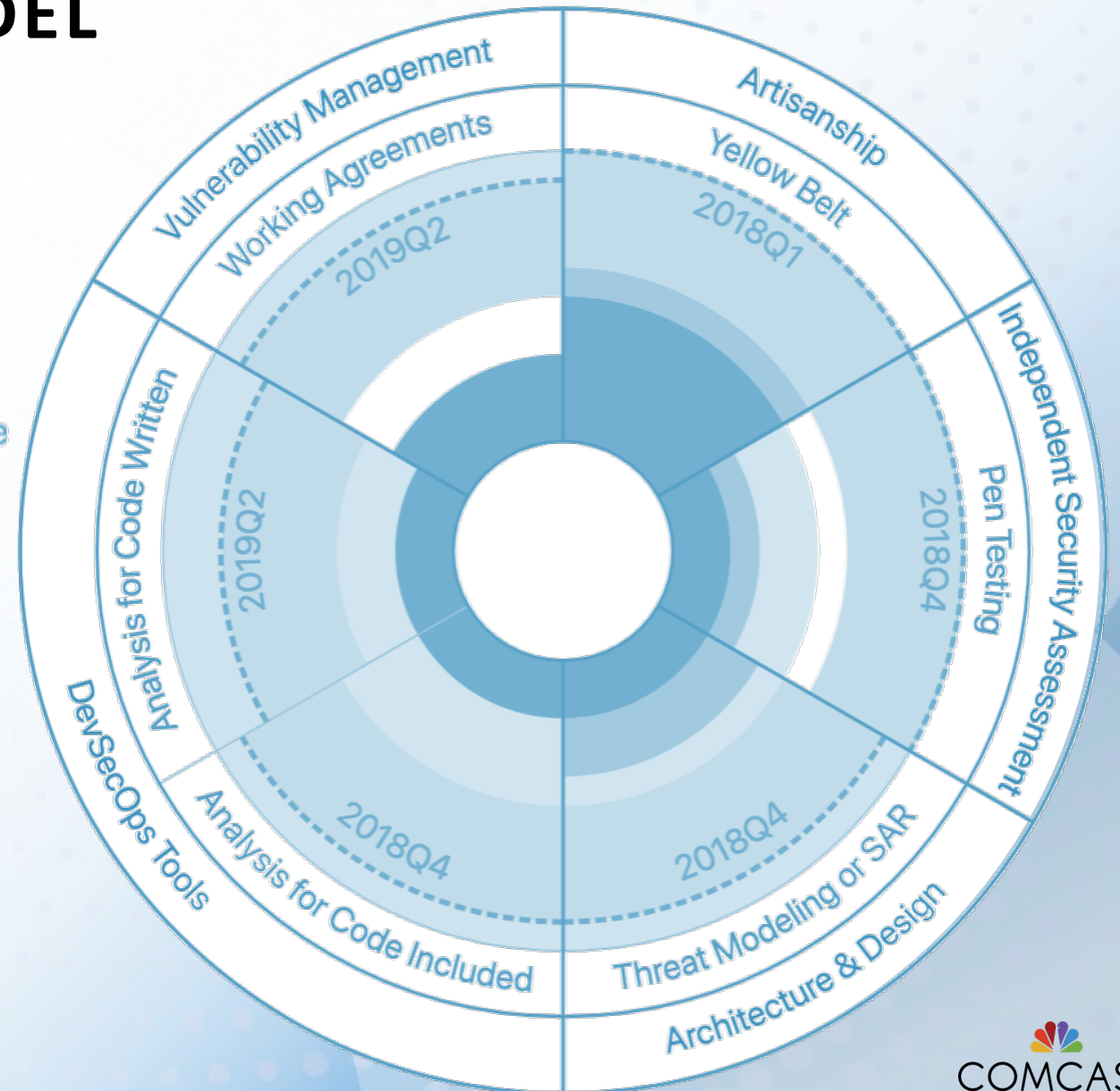




# SECURITY MATURITY MODEL

## EXAMPLE

- Culture** We have fully adopted this practice
- Actions** We're in the process of adopting this practice
- Words** We're making plans to adopt this practice
- Thoughts** We do not have plans for this practice
- Unknown** Unassessed or Needs follow up
- Trade-off** This practice is not worth it in this context



# THE COMCAST SECURITY GUILD

## MISSION

*To empower engineering teams to make good security decisions throughout the development process, In a way that members educate others on best practices, share knowledge, and collaborate on solutions, so that our products and services exceed our customer's expectations on security.*

## MEMBERSHIP LEVELS

Contributing  
Visiting  
Following  
Supporting  
Steering Committee

## ACTIVITIES

Professional Development  
Innovative Security  
Build Collaborative  
Platform  
Network  
Community Outreach -  
Annual Security by the  
Schuylkill conference



# TECHNOLOGIST TRAINING

## THE BELT SYSTEM

### LEVELS OF LEARNING AND DEVELOPMENT

Modeled after the popular belt-system in martial arts, the following four levels of learning are designed to take professionals along a journey from the most fundamental aspects of security to the most advanced.



#### **YELLOW BELT**

Comcast security philosophy, typical threats, and the ways we defend our customers and brand.

*90 min facilitated session  
or eLearning module*



#### **GREEN BELT**

Four journeys

1. Software
2. Network
3. Sys admin
4. DBA

*40 hours of technical Learn,  
Share, Do*



#### **BROWN BELT**

Advanced level, contributing and influencing security across Comcast.

*Specialized coursework and  
contributions*



#### **BLACK BELT**

1. Expert and/or specialized security knowledge.
2. Make significant contributions to Comcast and the industry.

*Executive nomination*



# COMCAST SECURITY CRAFTSMANSHIP MAKE RIGHT THING TO DO = EASY THING TO DO

**Autobahn**

**Secrets as a  
Service**

**Security  
Monkey**

**SSO Reverse  
Proxy**

**UScan**

**Raptor**

**Quest 365**

**Enterprise Key  
Management  
APIs**

**Comcast Code  
Signing APIs**

**RBA  
Microservices**

**Password of  
the Day**

**GitHub  
commit hooks**

# **TOP 10 PRACTICES SELECTED FOR GROUP GOALS**

**ANALYSIS FOR CODE YOU WRITE (SAST OR IAST)  
WORKING AGREEMENTS FOR DEVSECOPS TOOLS  
AND VULNERABILITY MANAGEMENT**

**ANALYSIS FOR CODE IMPORTED (SCA AKA OPEN  
SOURCE SECURITY)**

**SECRETS MANAGEMENT  
YELLOW BELT TRAINING**

**THREAT MODELING**

**PEN TESTING  
GREEN BELT**

**NETWORK-INITIATED SCANS**

**PSIRT PLAYBOOK  
FUZZING**

**ADOPTION IS  
SPREADING**



**ALL BUT ONE OF  
THE TEAMS  
ACHIEVED ALL  
OR ALMOST ALL  
GOALS BY  
REASSESSMENT**

**TOP “PLUSES” WE  
GET IN FEEDBACK  
AT END OF EACH  
SELF-  
ASSESSMENT**

**TEAMS SIGN UP FOR  
AVERAGE OF 2.46  
GOALS PER  
ASSESSMENT/  
REASSESSMENT. WE  
ASK FOR “1 OR 2,  
MAYBE 3”**

**THE PROGRAM IS WORKING**



“That was awesome!”, “Loved it!”, “Wow!”, “Very valuable and engaging. Much more than I expected”

“Very different approach than we expect from security”, “Dev team empowerment (teams own their own security)”, “Process driven by dev team priorities, not policy-driven”, “Collaborative effort to improve security”

Most valuable was... “Learning about all the different practices”, “Understanding the global view”, “Quantifying what needs to be done”

”Like it being facilitated for the first time”

“Loved the bang-for-the-buck ordering as opposed to a book of policies”

## TOP “EVEN BETTER IFS...” – AND FIXES

“[Wish] our chart didn’t look so red” – Switched to shades of green (or white, grey, or blue)

“[Wish] self-assessment or at least re-assessment was online” – In progress

“More on cloud and microservices” – In progress

”Make it easy to know who does what in security” – Security Catalog created

“More gradual on-ramp” – Light-green belt introduced

”Faster tool onboarding” – Staffing up

“Jargon like SCA, PCA, SAST, IAST confusing” – Changed to “Analysis for code imported” and “Analysis for code written”



COMCAST