RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-R03

Building an Android Scale Incident Response Process

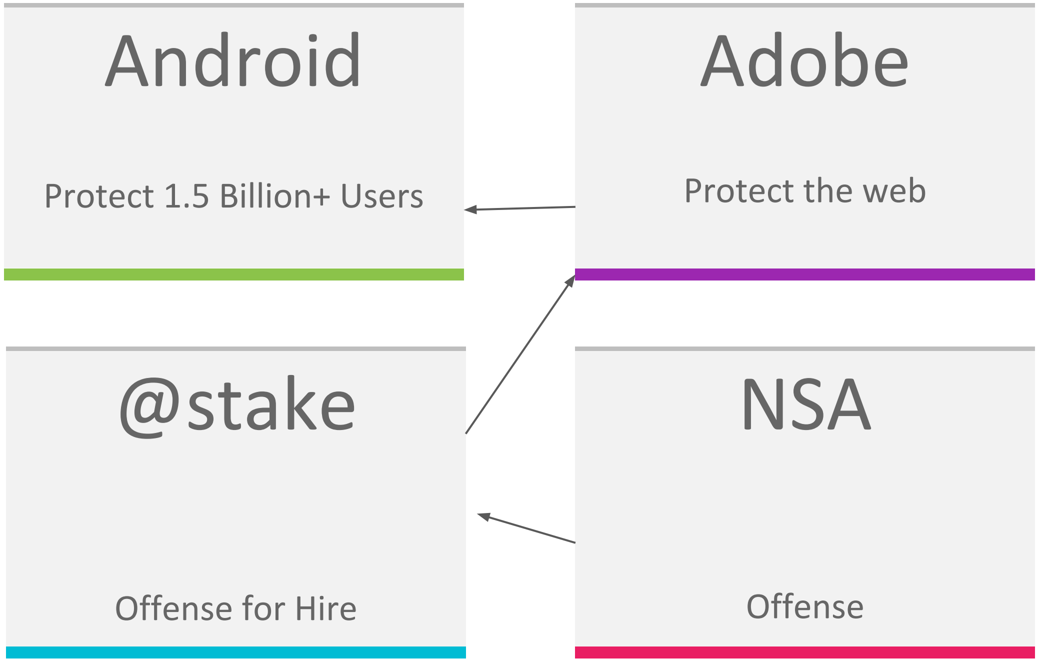
Adrian Ludwig

Lead - Android Security

Google

#RSAC

Who am I?



Android

Protect 1.5 Billion+ Users

Adobe

Protect the web

@stake

Offense for Hire

NSA

Offense

Goals

Describe strategies we’ve developed for incident response

Share thought process and lessons learned

Include Android-specific considerations (case studies)

The Incident Response Process

Establish Situational Awareness

Environment

Actors + Actions

Risks

Take Action

Accept Risk

Eliminate Risk

Manage the Risk

Data

The Android Ecosystem

1.5B+ Android 30DA Users	300M+ Users added in 2015	600+ New devices launched in 2015	50B+ App downloads in 2015

Actors

The Good

Google

- Security Team
- Product Engineering + QA
- PR / Communications
- Operations + Support
- Executives
- Legal

Ecosystem

- OEMs
- Carriers
- SOCs
- App Developers

The Bad

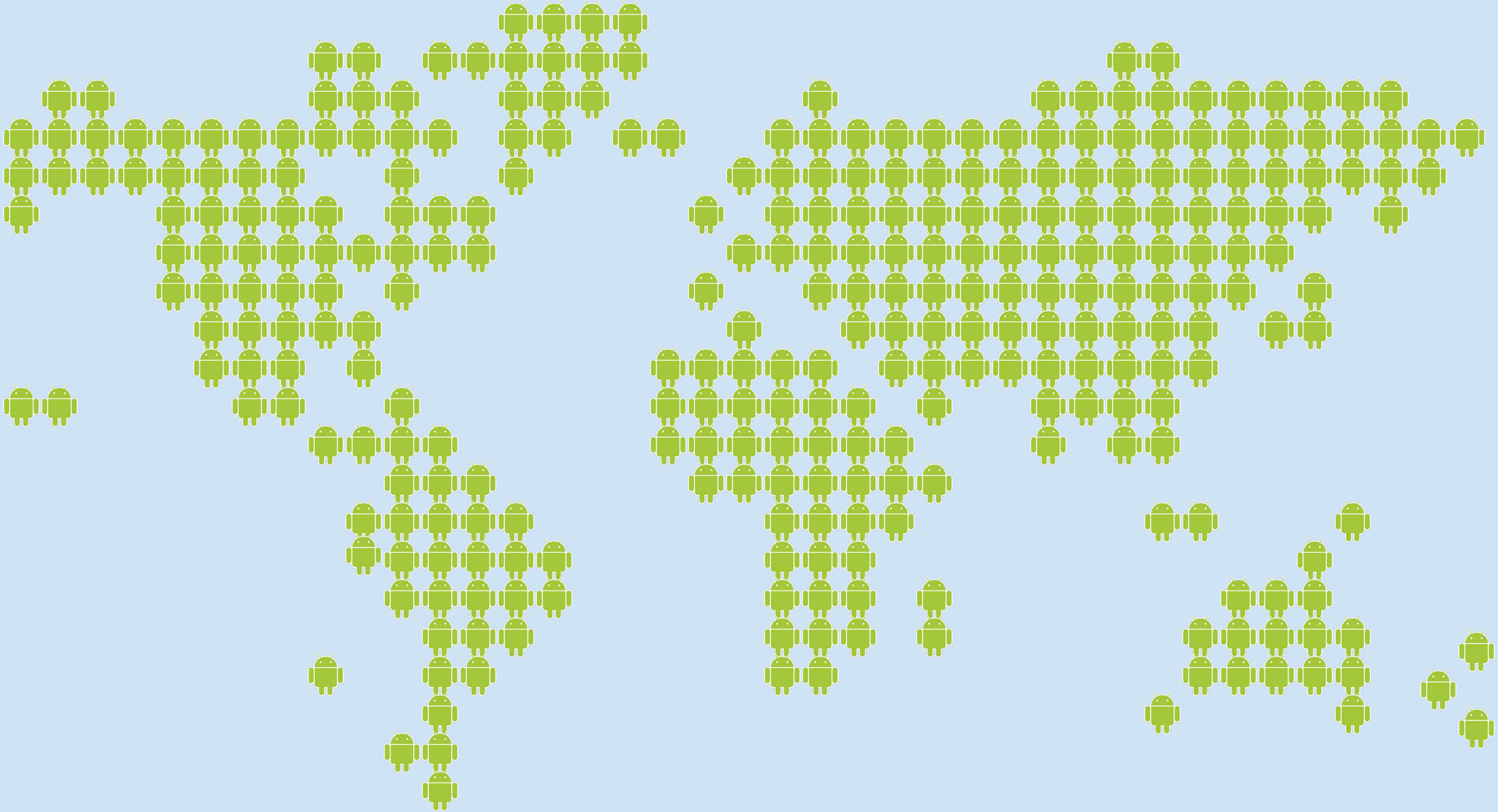
Attackers

- Attackers
- Malware Authors
- Thiefs
- Opportunists
- Network MITM

The Ugly

Complex Actors

- Consumers
- Enterprises
- Press
- Researchers
- Governments
- Security Companies



Threats

Malware

Vulnerabilities

Local Exploits

Hardware / Physical Attacks

Remote Exploits

Network Traffic Interception

Supply chain compromise

Data Sources

Google Play

Safebrowsing for Chrome

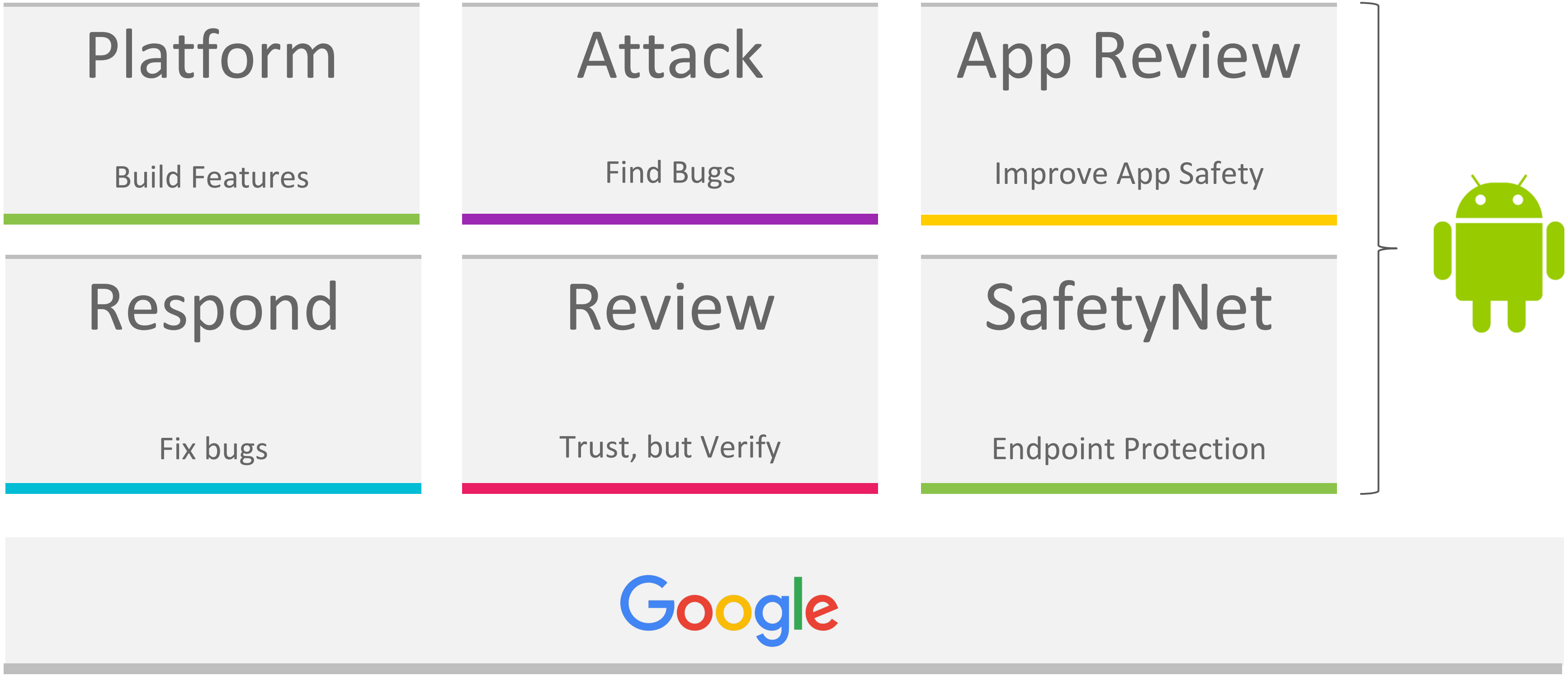
Verify Apps

Android Safety Net

Android Device Manager

Billions of new pieces of data including apps, developers, app behavior, relationships, and third-party analyses are added every day.

Organization



Platform

Build Features

Attack

Find Bugs

App Review

Improve App Safety

Respond

Fix bugs

Review

Trust, but Verify

SafetyNet

Endpoint Protection

Google

Responses

Google Public Statement

Google Play Update

Google Service Update (Verify Apps, SafetyNet)

Patch to AOSP

Warn users

Joint statement with partners

Major 3rd Party App Patch

Publish Research

Change an API

Patch a Google app

Publish a best practice

3rd Party Apps (Google Play)

Ecosystem Wide patch delivery

3rd Party App Upgrade

Release a major update

Nexus Update

Warn developers

And many more...

Strategy Lenses

Frequency

How often is the threat realized?

Velocity

How quickly is a threat realized?

Impact

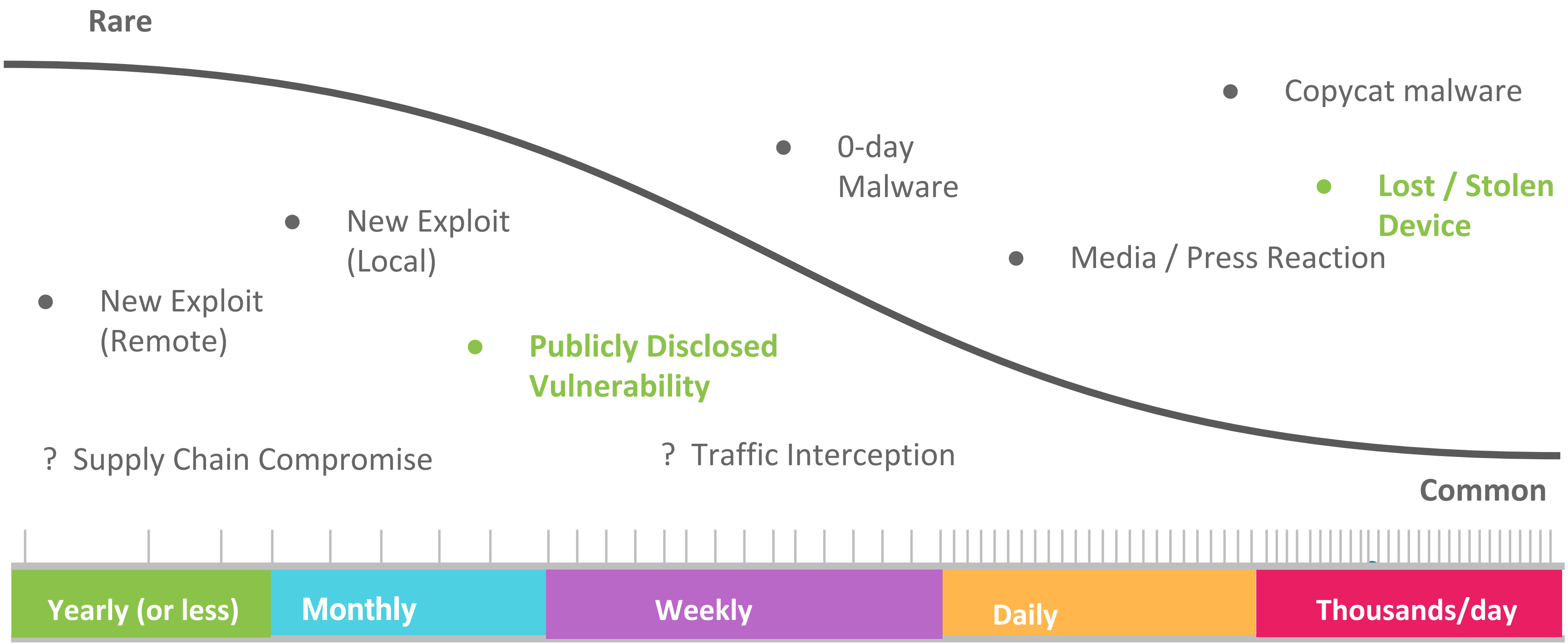
What happens if a threat is realized?

Scope

What portion of the ecosystem is at risk?

Incident Frequency

Incident Frequency



Rare

- New Exploit (Remote)
- New Exploit (Local)
- **Publicly Disclosed Vulnerability**
- 0-day Malware
- Media / Press Reaction
- Copycat malware
- **Lost / Stolen Device**

? Supply Chain Compromise

? Traffic Interception

Common

Strategies to Reduce Frequency

Change the attacker economics

Move the target

“Smart phone thefts rose to 3.1 million in 2013”

Source: Consumer Reports

Responses

React

Device Manager

“Find my phone”

“Lock my phone”

“Wipe my phone”

Prevent

Lockscreen

Encryption

Factory Reset Protection

2.5 Million Monthly Users of Device Manager “Find my Phone”

Lockscreen usage up 50% between 2014 and 2015 Nexus devices

Encryption and FRP Enabled by default

Smart phone thefts declined from 3.1 in 2013 to 2.1 million in 2014

Source: Consumer Reports

nexus

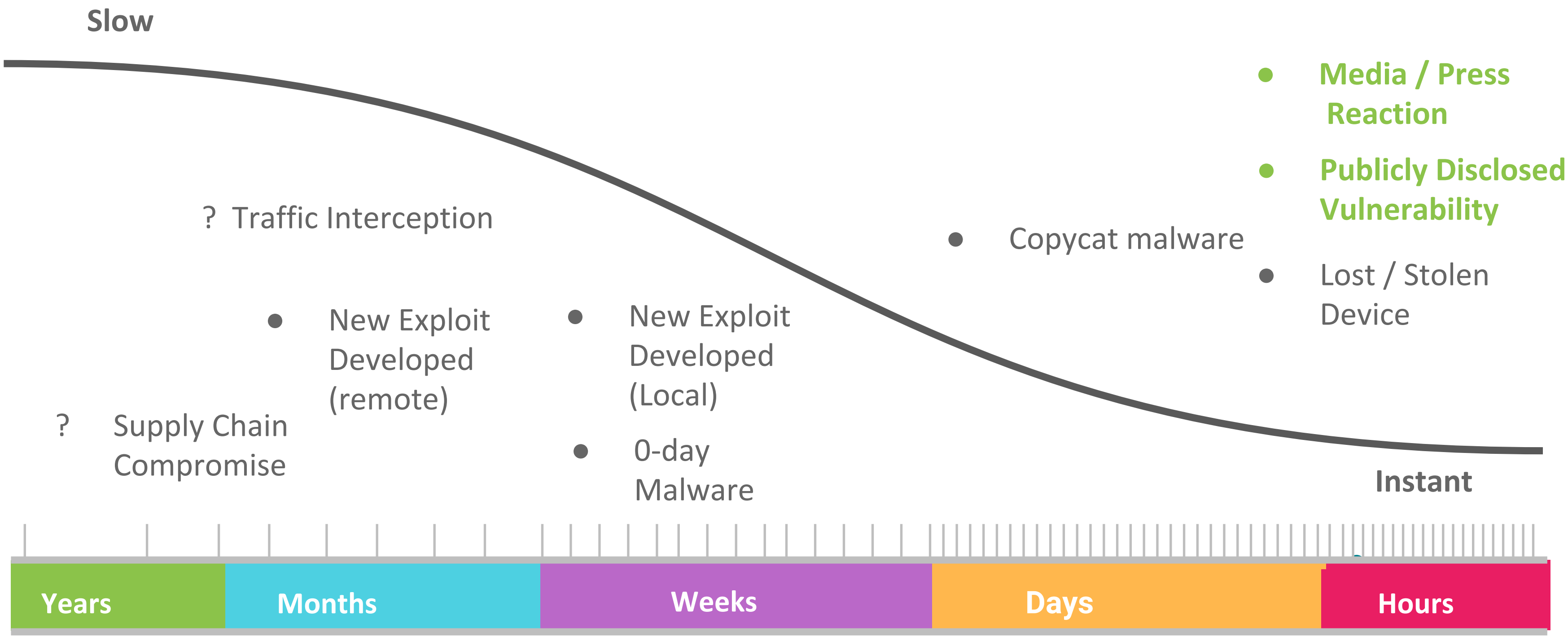
g.co/AndroidSecurityRewards

$200,000 paid in 2015

Up to $38,000
per security issue

Incident Velocity

Incident Velocity



? Traffic Interception

? Supply Chain Compromise

- New Exploit Developed (remote)
- New Exploit Developed (Local)
- 0-day Malware
- Copycat malware
- **Media / Press Reaction**
- **Publicly Disclosed Vulnerability**
- Lost / Stolen Device

Strategies to Reduce Velocity

Centralize your response

Batching and Cadence

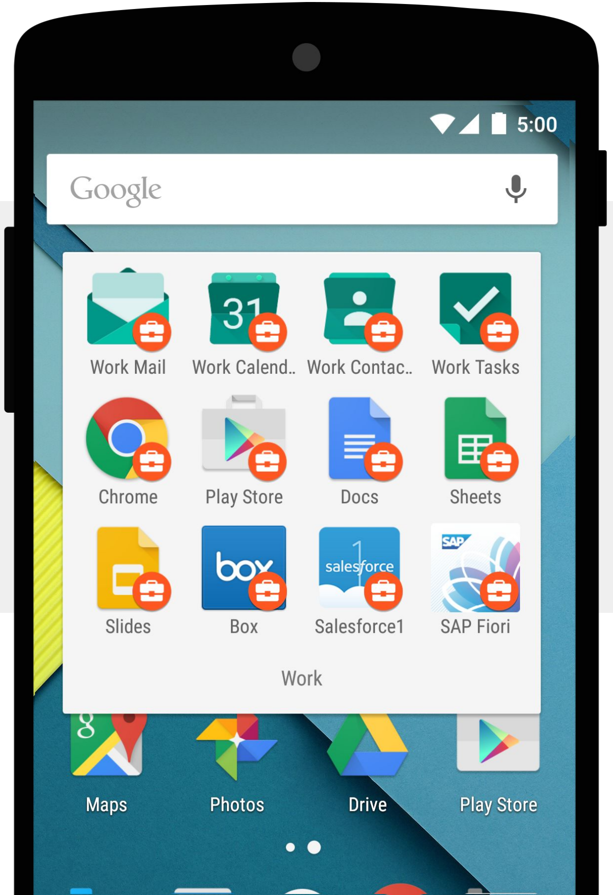
Quality and Automation

nexus

Monthly Security Updates

Monthly Security Bulletins

3 years from device availability



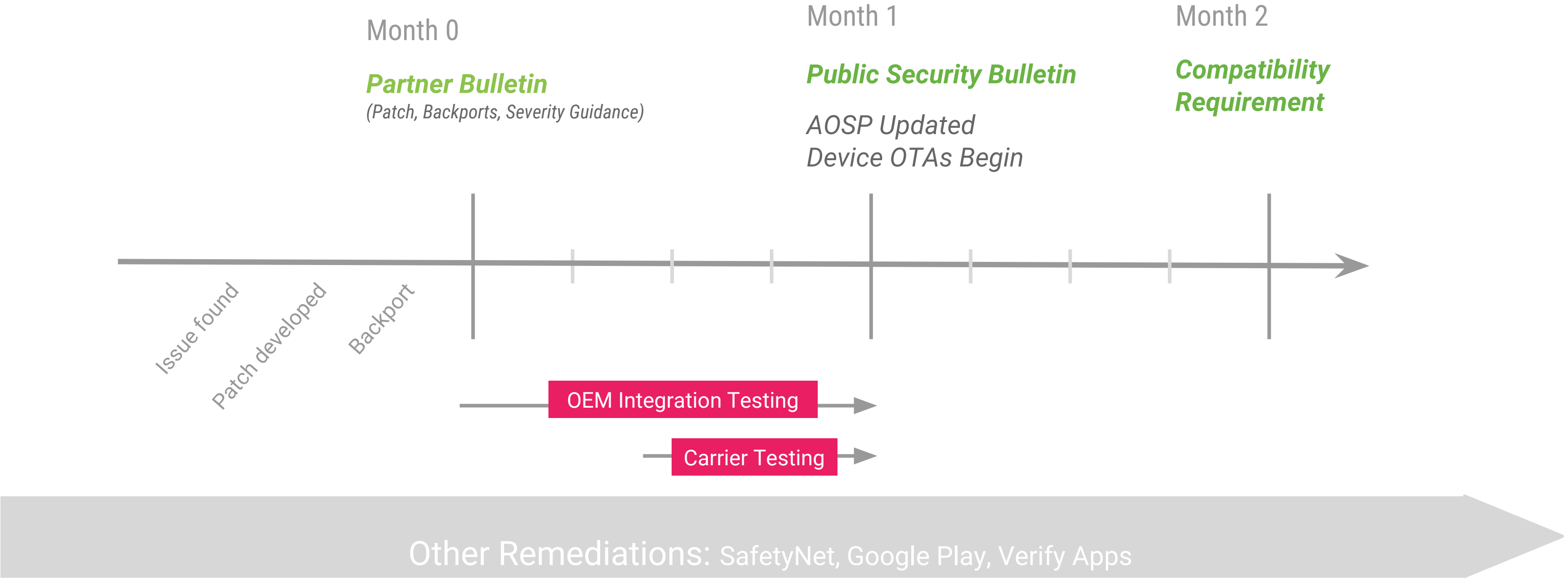
Google

SAMSUNG

LG

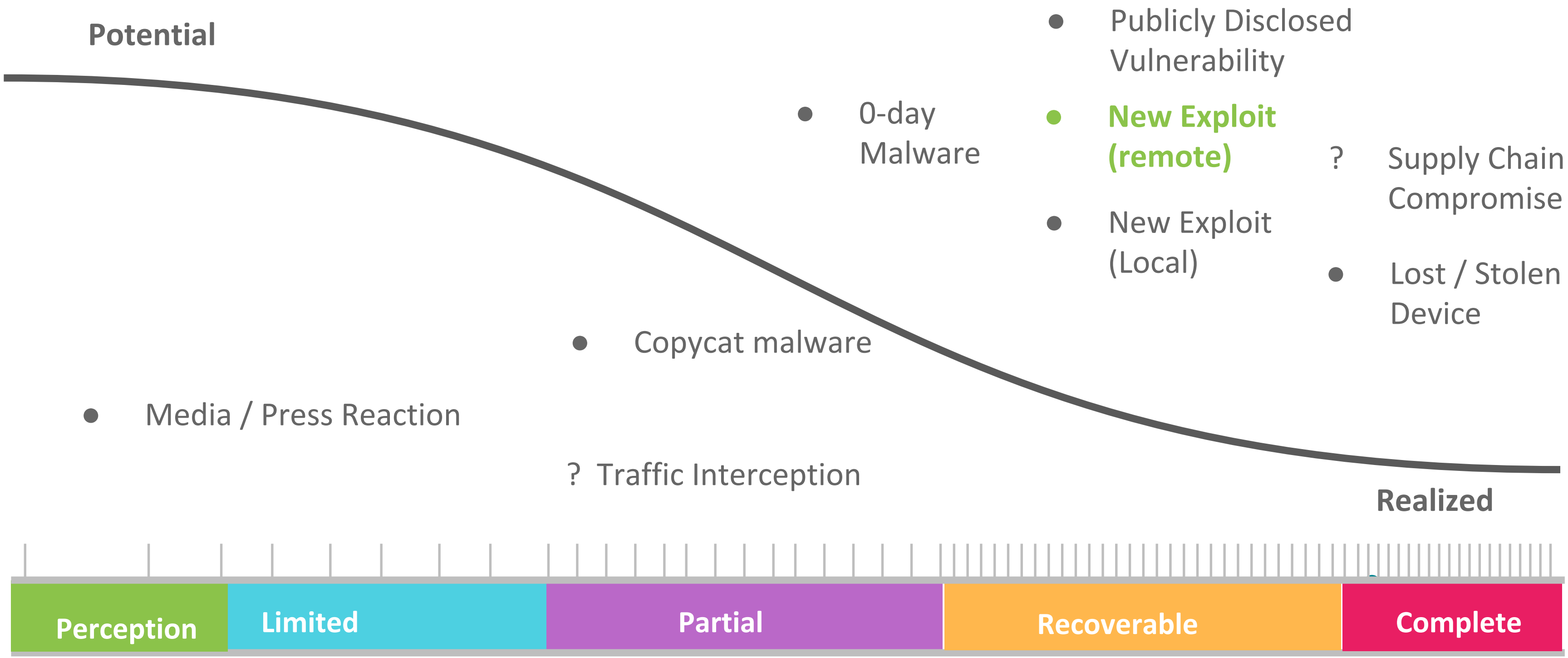
BlackBerry

Android Security Monthly Process



Incident Impact

Incident Impact



Potential

● Publicly Disclosed Vulnerability

● 0-day Malware

● **New Exploit (remote)**

? Supply Chain Compromise

● New Exploit (Local)

● Lost / Stolen Device

● Copycat malware

● Media / Press Reaction

? Traffic Interception

Realized

Perception	Limited	Partial	Recoverable	Complete

Strategies to Reduce Impact

Provide a safer path

Isolate high risk components

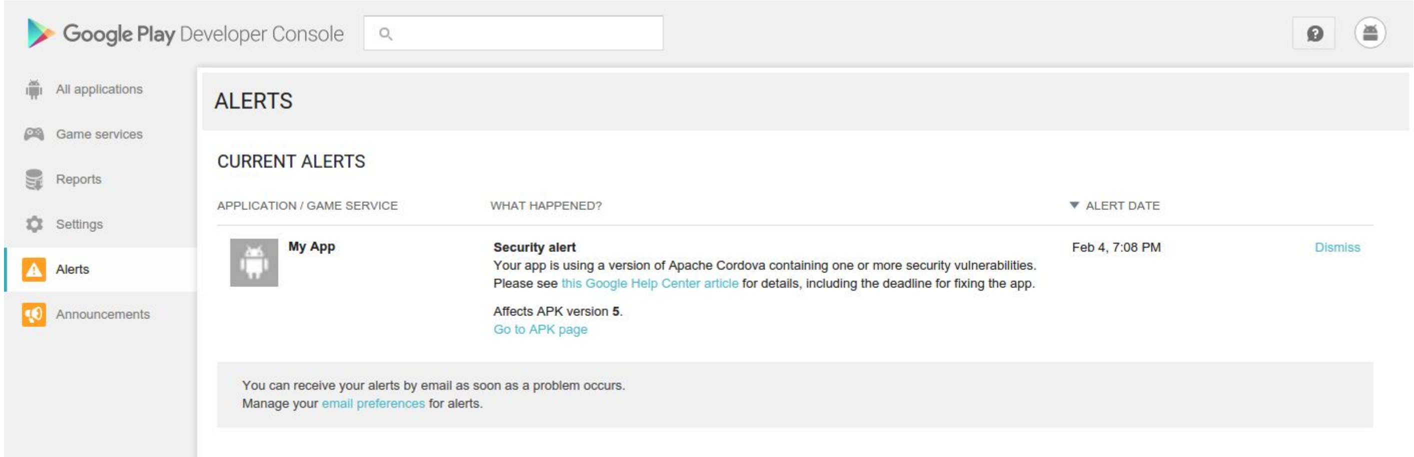
Focus on recovery

Developer APIs

```
SecurityProvider :
GmsCore_OpenSSL

SafetyNetApi.attest
```

Developer Security Warnings



ALERTS

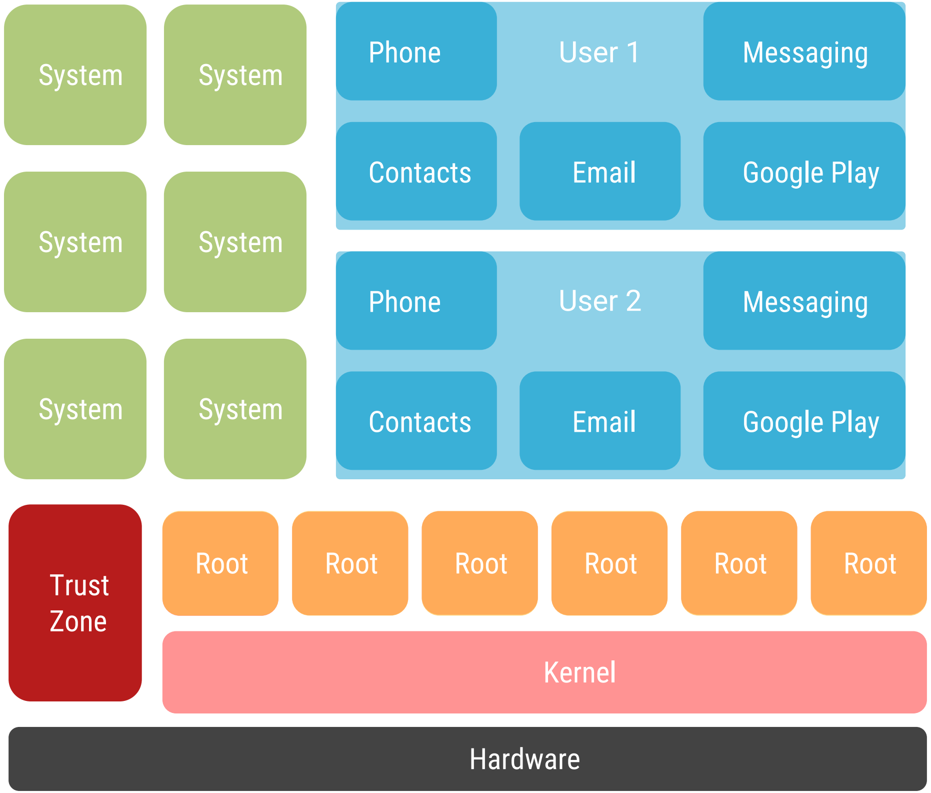
CURRENT ALERTS

APPLICATION / GAME SERVICE	WHAT HAPPENED?	▼ ALERT DATE	
My App	**Security alert** Your app is using a version of Apache Cordova containing one or more security vulnerabilities. Please see this Google Help Center article for details, including the deadline for fixing the app. Affects APK version **5**. Go to APK page	Feb 4, 7:08 PM	Dismiss

You can receive your alerts by email as soon as a problem occurs.
Manage your email preferences for alerts.

85% Reduction in Installs of Vulnerable Apps in 2015

Isolation at every level



System System

System System

System System

Phone User 1 Messaging

Contacts Email Google Play

Phone User 2 Messaging

Contacts Email Google Play

Trust Zone

Root Root Root Root Root Root

Kernel

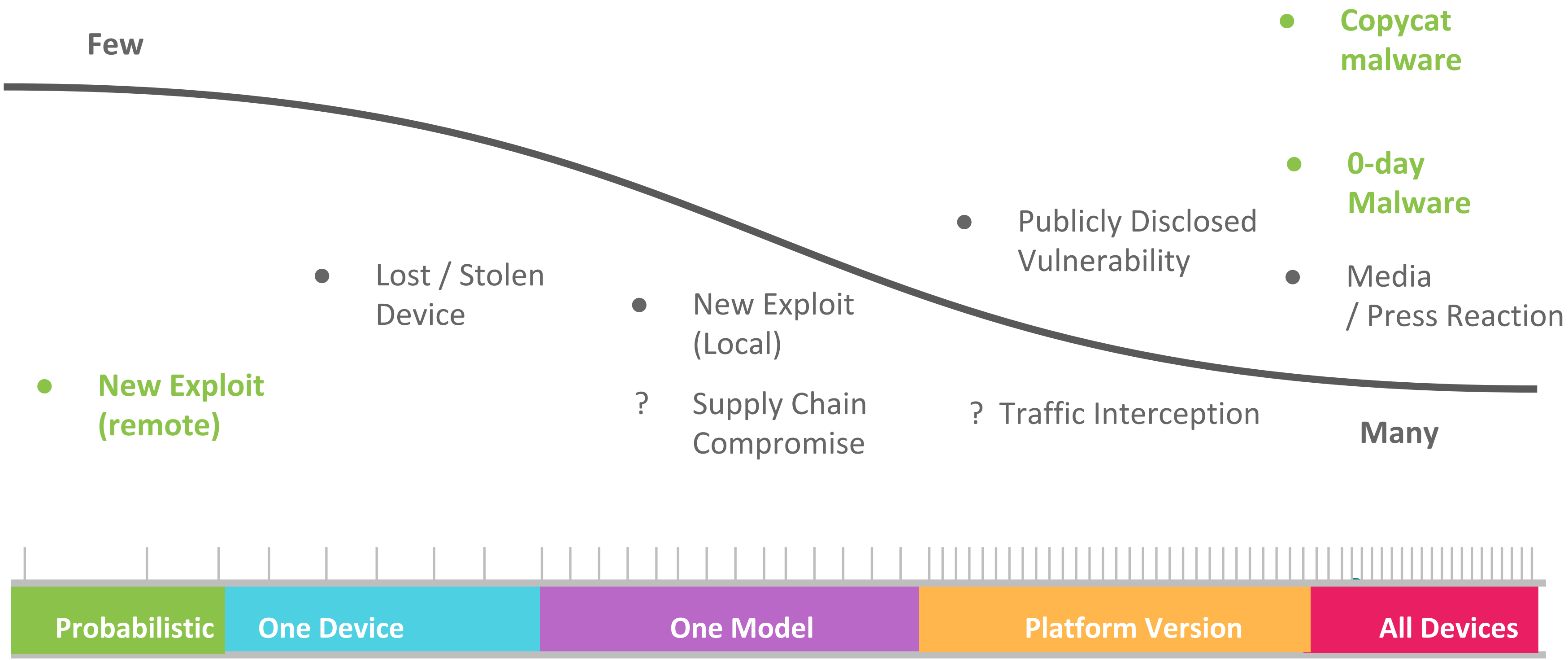
Hardware

Focus on recovery

Verified Boot + SafetyNet = ❤

Incident Scope

Incident Scope



Few

● New Exploit (remote)

● Lost / Stolen Device

● New Exploit (Local)

? Supply Chain Compromise

● Publicly Disclosed Vulnerability

? Traffic Interception

● Copycat malware

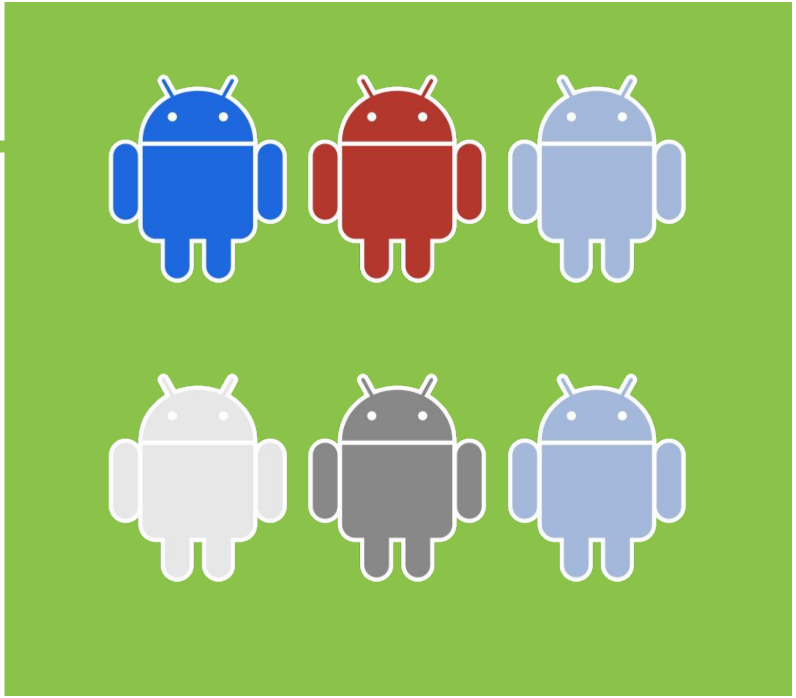
● 0-day Malware

● Media / Press Reaction

Many

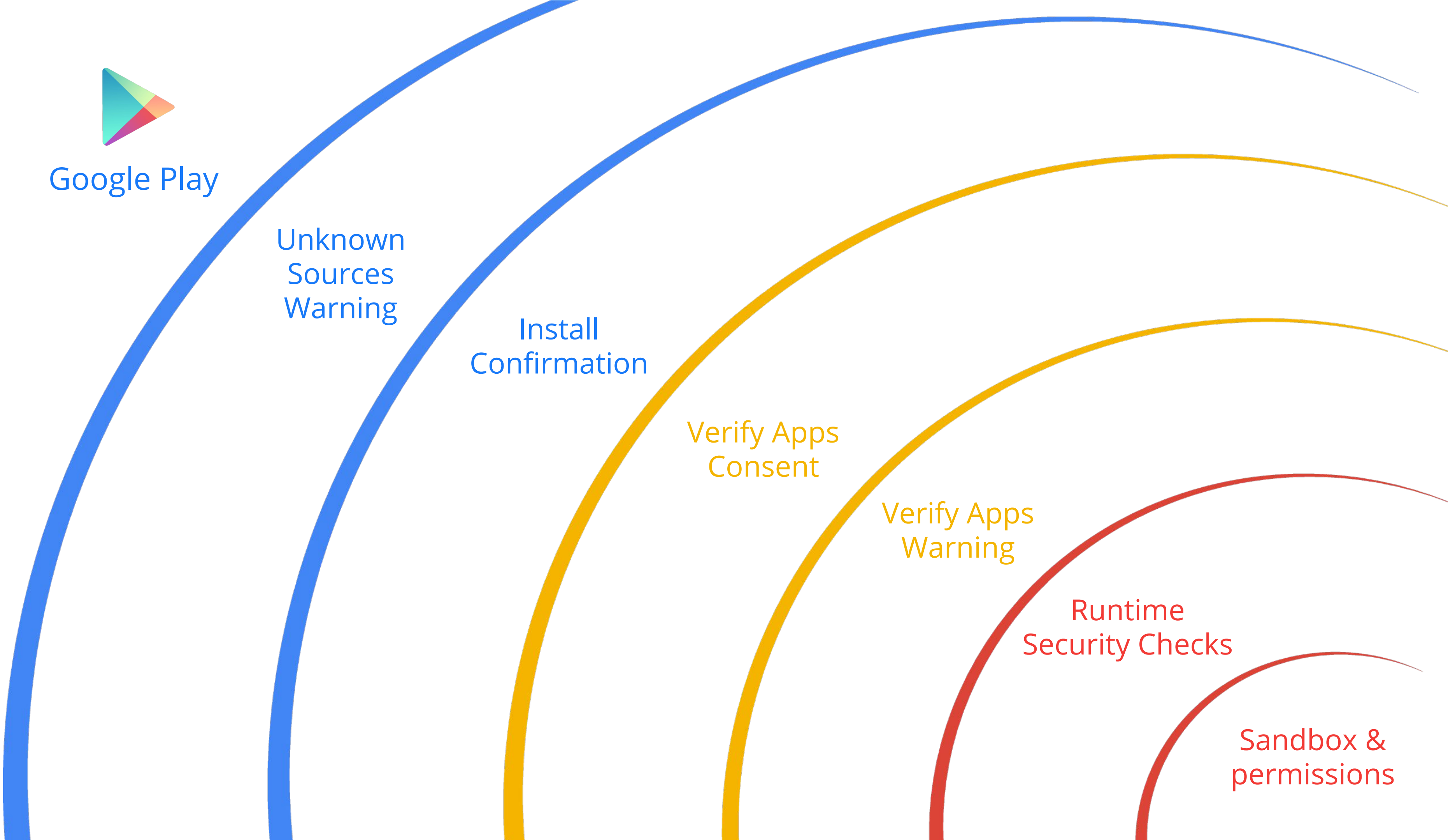
Probabilistic | One Device | One Model | Platform Version | All Devices

Reduce Incident Scope



Add Speed Bumps

Embrace diversity



Google Play

Unknown Sources Warning

Install Confirmation

Verify Apps Consent

Verify Apps Warning

Runtime Security Checks

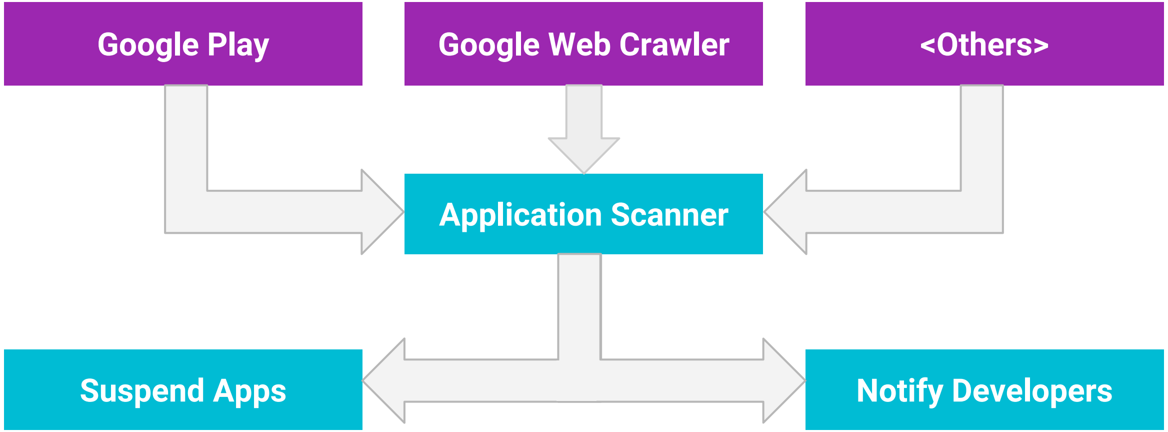
Sandbox & permissions

Application Review

Collect Apps

Analyze Apps

Enforcement



Application scanner details

Static analysis

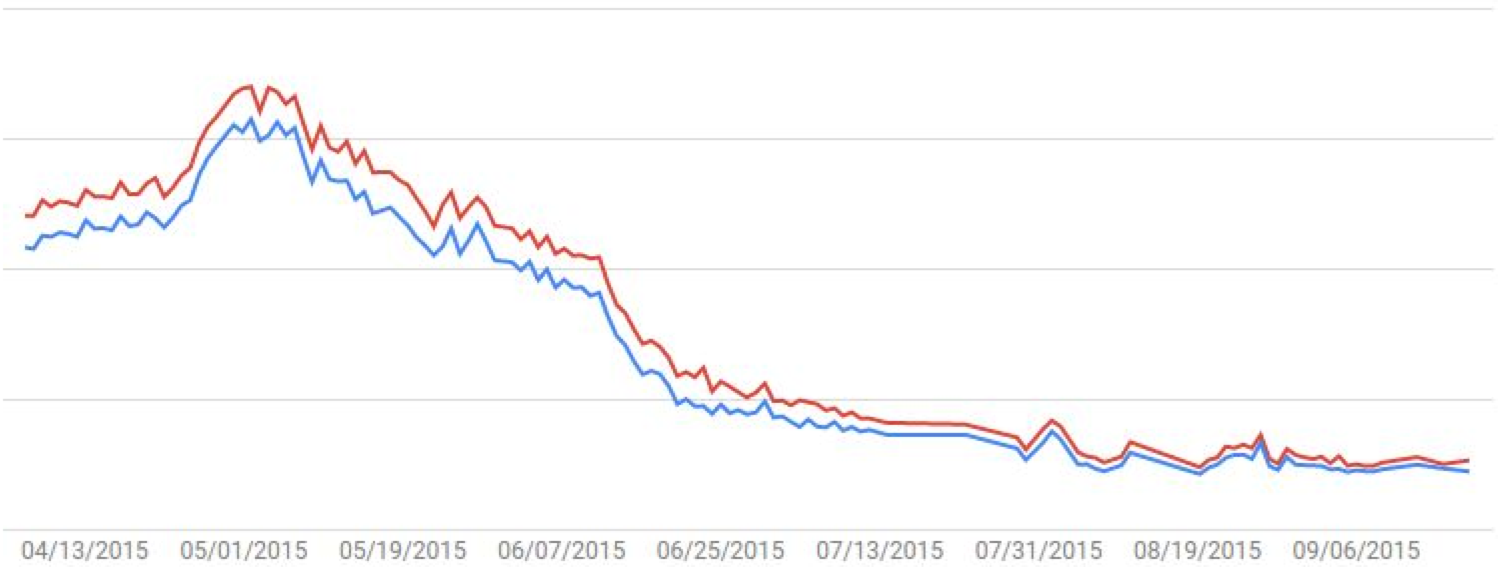
Dynamic analysis

Machine learning

Intelligence-based discovery

Signature-based discovery

80% Reduction of Russian Bank Phishing Trojans



Infected devices in Russia
Infected devices worldwide

Embrace Diversity

Intentional

ASLR

Update Frequently

Natural

OEM

SOC

Hardware Architecture

Build Time Changes

Predicting “real” scope is hard

Vulnerability	Initial Claim Headline	Unique APKs	Peak exploitation after public release (per install)	Exploitation before public release (absolute)
Master Key	99% of devices vulnerable	1231	< 8 in a million	0
FakeID	82% of Android users at risk	258	<1 in a million	0
Stagefright	95% of devices vulnerable	N/A	None confirmed	N/A

Source: Google Safety Net Data; Masterkey data collected from 11/15/2012 to 8/15/2013 and previously published at VirusBulletin 2013. Fake ID data collected data collected from 11/15/2012 to 12/11/2014 and previously published at the RSA Conference 2015. Stagefright data current through February 2016.

To recap

Strategy Lenses

Frequency

Use economics
Change the target

Velocity

Centralize
Batch and Cadence
Automate

Impact

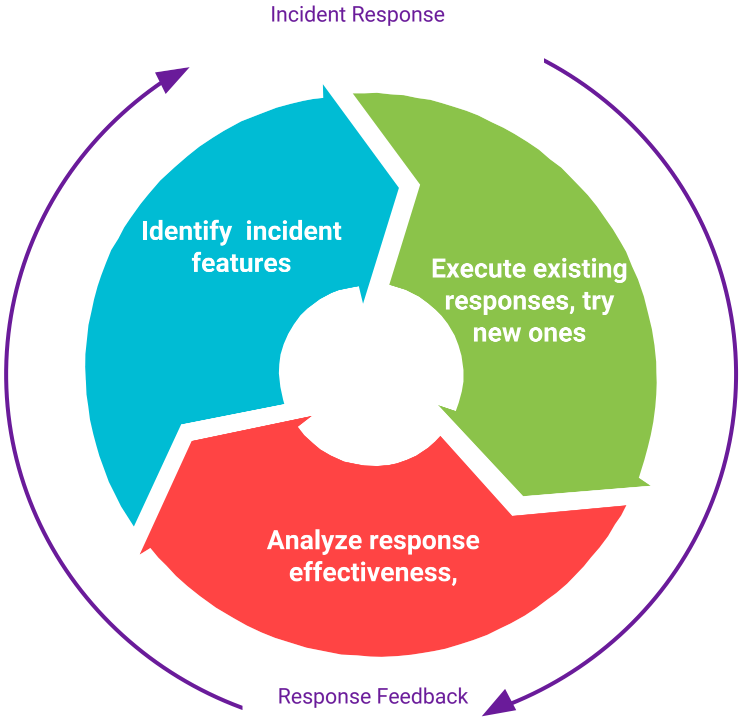
Another Path
Isolation
Recovery

Scope

Speed Bumps
Diversity

Key Learnings

- Use data as your source of truth (not stories!)
- Look for new responses (think offensively!)
- Try not to get lost in the details (this is hard!)



Incident Response
Identify incident features
Execute existing responses, try new ones
Analyze response effectiveness,
Response Feedback

Thank You!

aludwig@google.com