SECURITY INNOVATION

Building a Collaborative & Social Application Security Program

Joe Basirico VP of Services

October 5th 2017

SECURITY INNOVATION

We help our customers reduce their application security risk through

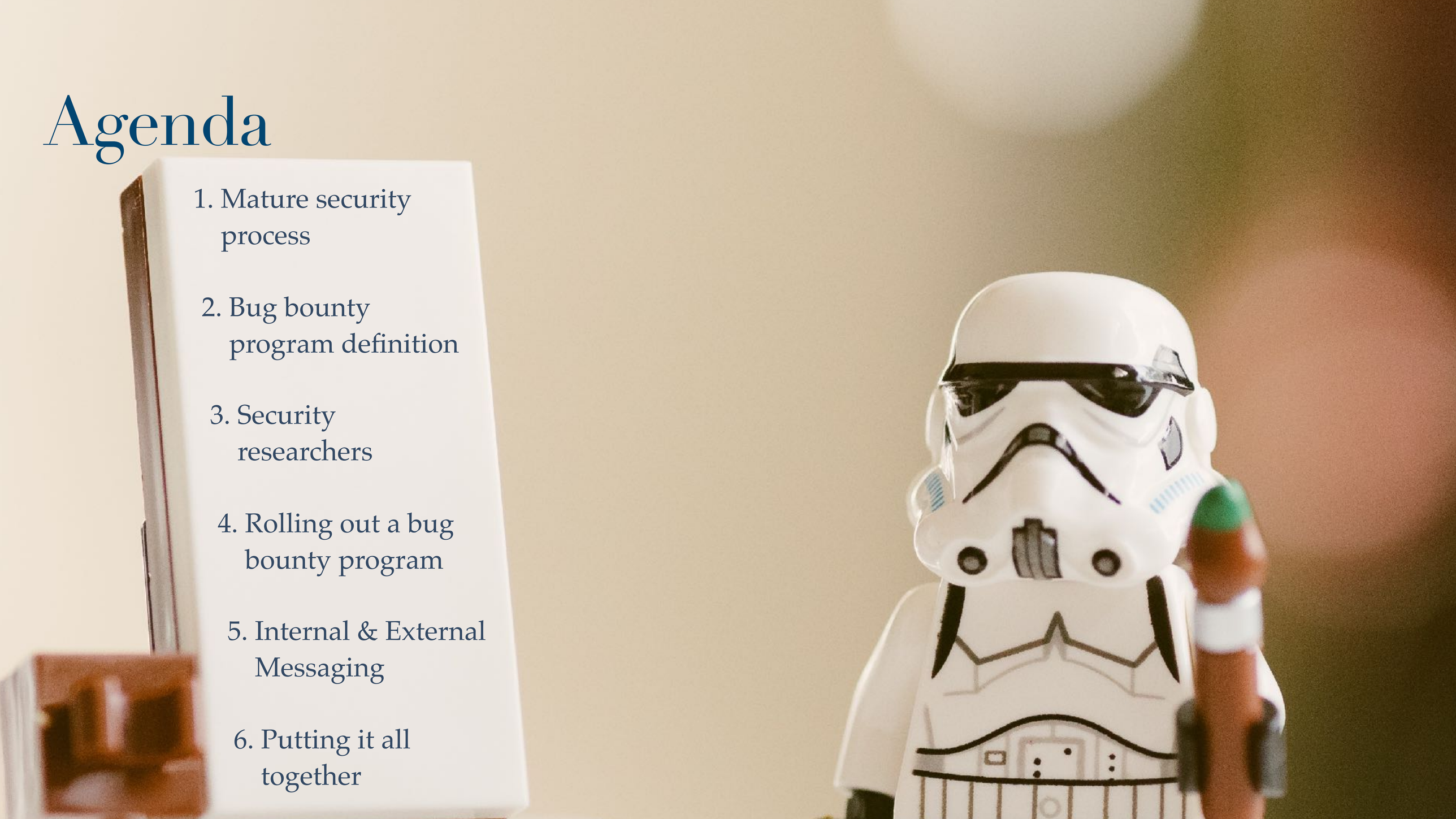
Education

Assessment Services

Process Guidance

Agenda

1. Mature security process
2. Bug bounty program definition
3. Security researchers
4. Rolling out a bug bounty program
5. Internal & External Messaging
6. Putting it all together



Application Security Maturity Timeline

Table Stakes

External Messaging → Automated Scan (Tools) → External Assessment #1 → Security Training

Internal

Internal Review → Bug Bash → Security Team Creation → Revise External Messaging

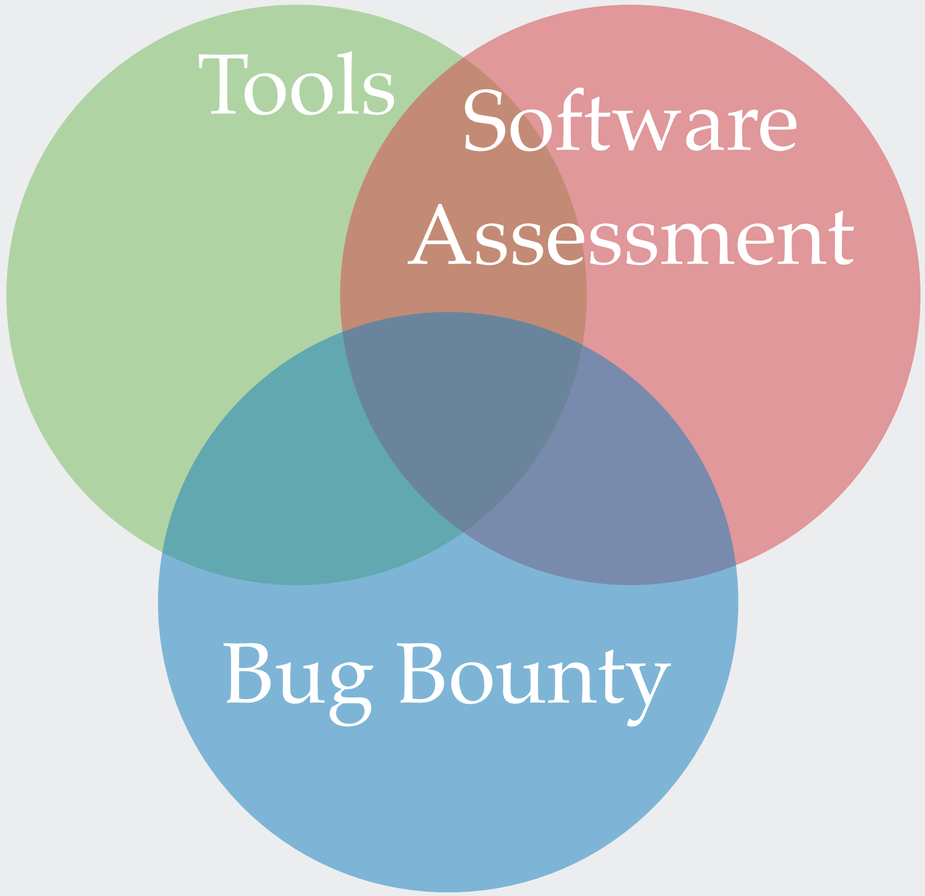
External

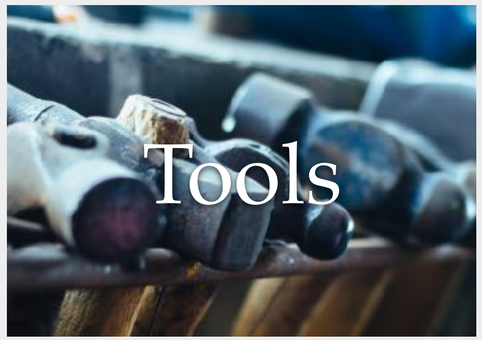
SDL Gap Analysis → External Security Assessment #2 → Fix/Re-test → Bug Bounty Program

SECURITY INNOVATION

Key SLDC Components

- ✓ Reactive Guidance & Proactive Training
- ✓ Internal Security Team
  - ✓ Security Lead (CISO, Guru, Tzar)
  - ✓ Security Review Team / Risk Assessment Team
- ✓ External Assessment
- ✓ Compliance & Data Risk Categorization and Discovery





Start here:

- Types: SAST, DAST, WhiteHat
- Good for low hanging fruit
- Table stakes

Next Steps:

- Shore up base level security
- Security Training
- Internal review of common issues

What to do:

- Types: Pen Test/Code Review
- Deep Vulnerabilities
- What does secure look like

Next Steps:

- Respond to critical-med issues
- Address & Retest
- Train using findings, no repeats

Value:

- Missed Basic Vulnerabilities
- Expert Critical Issues

Next Steps:

- Revise internal processes
- Revise BBP
- Revise Rewards

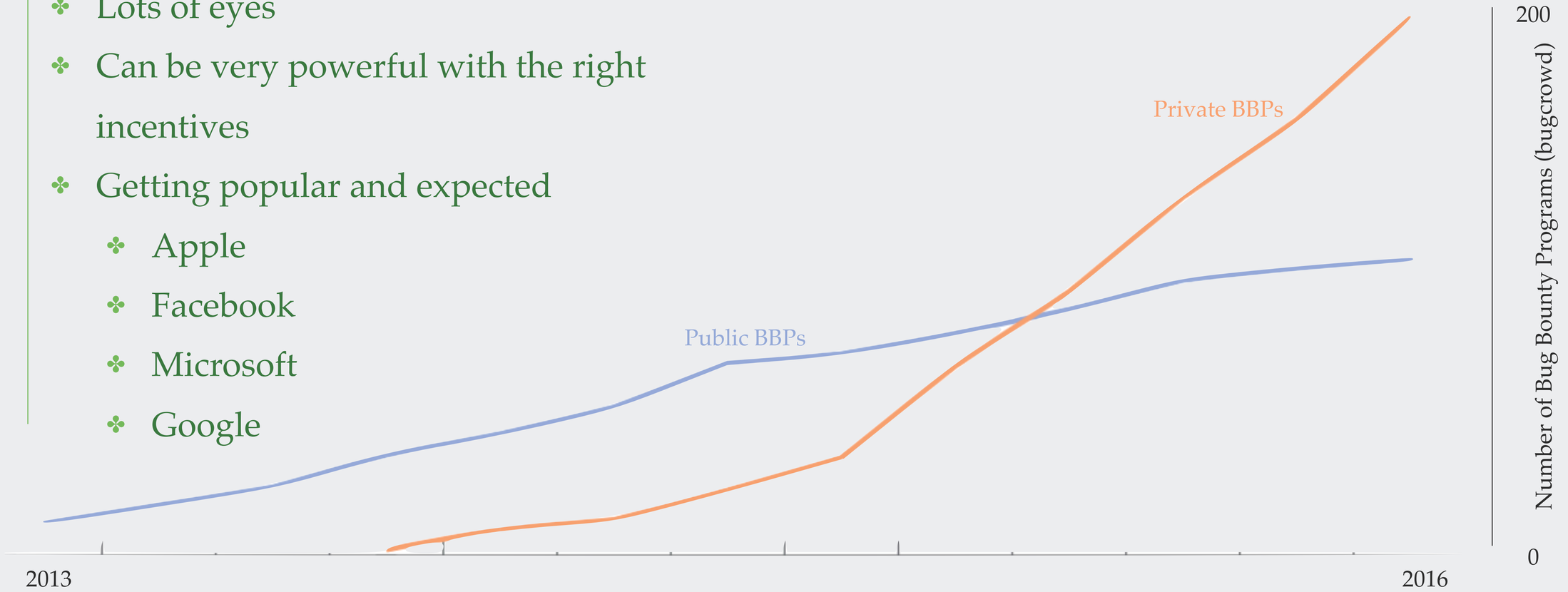
Bug Bounty Programs

Recognition & compensation for responsibly reporting bugs

SECURITY INNOVATION

Strengths

- Lots of eyes
- Can be very powerful with the right incentives
- Getting popular and expected
  - Apple
  - Facebook
  - Microsoft
  - Google



Bug Bounty Programs

Recognition & compensation for responsibly reporting bugs

SECURITY INNOVATION

Strengths

- Lots of eyes
- Can be very powerful with the right incentives
- Getting popular and expected
  - Apple
  - Facebook
  - Microsoft
  - Google

Weaknesses

- Can be overwhelming
  - Invalid report submissions
  - Timely response required
  - Incentive to submit and see what sticks
- Can open you up to poor publicity
- Scoping issues

Bug Bounty Programs

Recognition & compensation for responsibly reporting bugs

SECURITY INNOVATION

Strengths

- Lots of eyes
- Can be very powerful with the right incentives
- Getting popular and expected
  - Apple
  - Facebook
  - Microsoft
  - Google

Weaknesses

- Can be overwhelming
  - Invalid report submissions
  - Timely response required
  - Incentive to submit and see what sticks
- Can open you up to poor publicity
- Scoping issues

Conclusion: Important part of a mature secure process; roll it out when you're prepared

What Security Researchers Want

SECURITY INNOVATION

Respect

- Professional Security Researchers
- Giving you free testing
- Motivations can vary, but are not malicious

Rewards

- SWAG/Cash
- Interview Opportunity
- …more on this later

Results

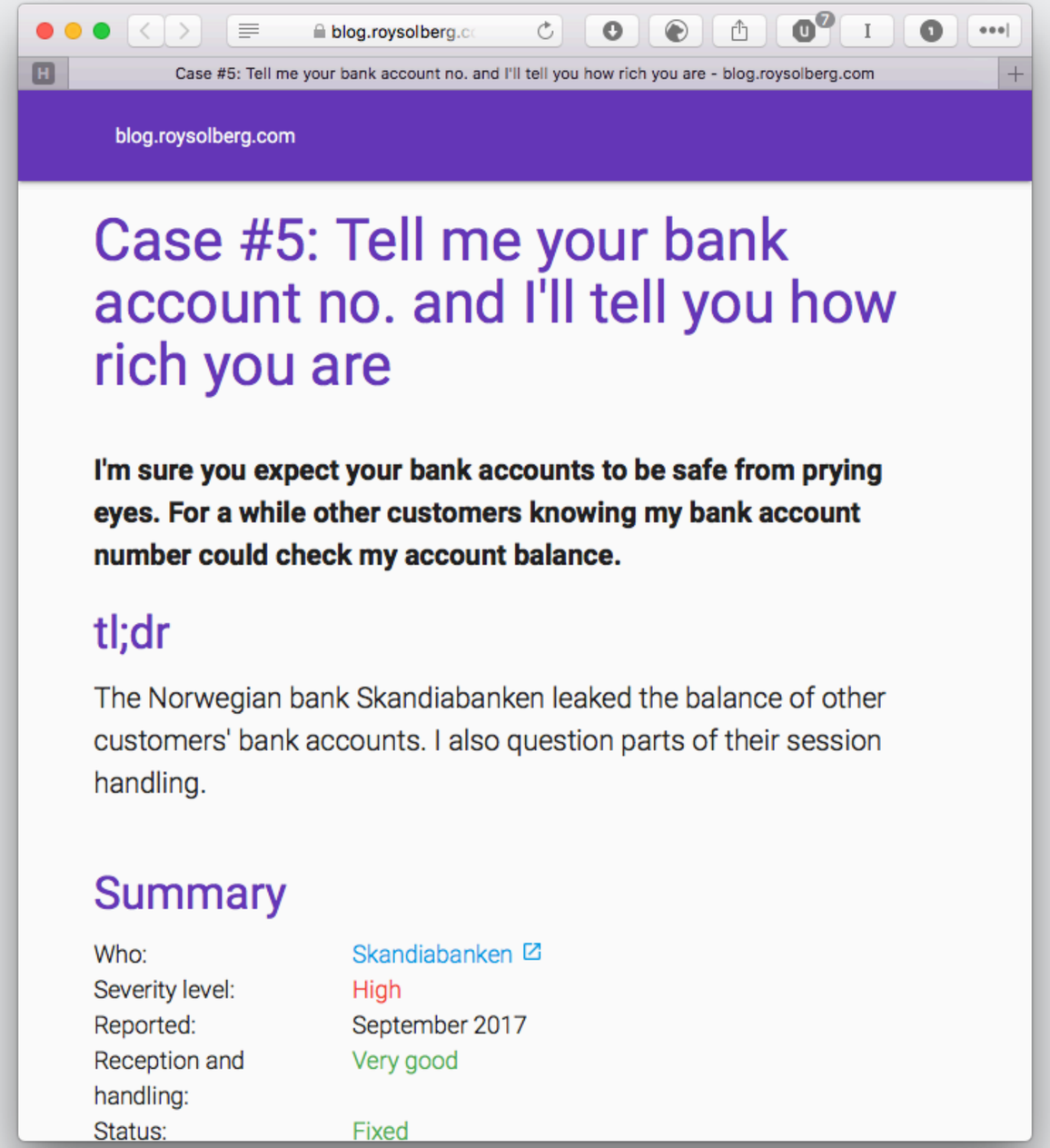
- Set expectations for progress and response
- Create a secure line of communication
- Follow up! Do not drop the ball
  - When will the issue be resolved?
  - Will they need to verify the fix?
  - When will they receive their reward?

Recognition

- Disclosure and public messaging
- How will you let your users know about the issue
- Acknowledgement & credit
- …more on this later

Disclosure Options

- No Disclosure - highest bidder
  - Immediate Release
- Open Disclosure
  - Immediate Release
- Responsible Disclosure
  - Ever to be released?
  - Hard / Negotiable Timeline



Assume Communications Are Public

Instagram's "Million Dollar Bug"

- Researcher felt slighted by Facebook's response
- Wrote multi-page blog post about technical details and all communication interactions

Based on the interactions experienced to date with Facebook's security team, decision is made to publish findings.

Dec 4

AWS Keypairs From sensu.instagram.com Rejected

Dec 1

Alex Stamos Phones My Employer

Late in the evening, Facebook's CSO, Alex Stamos, contacts the CEO of the company I work for. Alex explains the possibility of legal and criminal actions if I do not comply with their demands, which include keeping all findings secret.

Dec 1

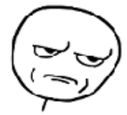
AWS Keypairs From sensu.instagram.com Reported

With no real clarification as to how the rules at https://www.facebook.com/whitehat were being interpreted, AWS keypairs and S3 bucket access was reported as a third and final vulnerability to Facebook's Whitehat program.

Facebook contacts me via the normal security support system. Facebook states 'We feel it's appropriate for you to write up your process for finding and testing the initial RCE on sensu.instagram.com, but not any actions you took after finding that RCE.'

Dec 1

Weak Accounts on sensu.instagram.com Rejected - User Privacy Violation Claimed



Nov 16

RCE in sensu.instagram.com Accepted For $2,500

Facebook acknowledges this vulnerability, but splits it with my friend who originally found the server. Facebook states 'typically only reward the first researcher to report a valid issue to us through the bounty program, but in this case, we will be paying for related reports with different information that helped us track down and fix this issue.'

After numerous messages back and forth with Facebook, and having my security support case closed multiple times, Facebook finally gives the reason of 'user privacy violation' for rejecting this vulnerability.

Oct 28

Clarification Requested Regarding Testing Scope

Over the course of several weeks I sought to understand why the written rules were different than the rules stated by Facebook's security team. This was never clearly resolved.

Oct 28

Response Received Regarding Weak Accounts on sensu.instagram.com

The response from the Facebook security team implies that I have gone outside the scope of the Whitehat bounty program. No explanation is given for what about my vulnerability submission is out of scope.

Oct 24

AWS Keypair From sensu.instagram.com Discovered and Tested

While waiting for a reply from Facebook security regarding weak accounts, examined sensu.instagram.com configuration further and discovered AWS keypair. Keypair was discovered to provide access to a second keypair, and thus to 80 different Amazon S3 buckets.

Oct 24th?

sensu.instagram.com Taken Offline or Firewalled

Around Oct 24th, remote access to this server is no longer possible.

Oct 22

Weak Accounts on sensu.instagram.com Reported

Weak accounts reported as a vulnerability to Facebook's Whitehat program.

Oct 22

RCE in sensu.instagram.com Acknowledged

Facebook confirms that they are investigating this vulnerability.

Oct 21

Weak Accounts on sensu.instagram.com Discovered

Local Postgres DB for Sensu-Admin is accessed to enumerate accounts. 60 employee accounts are discovered, with at least 12 having extremely weak passwords set.

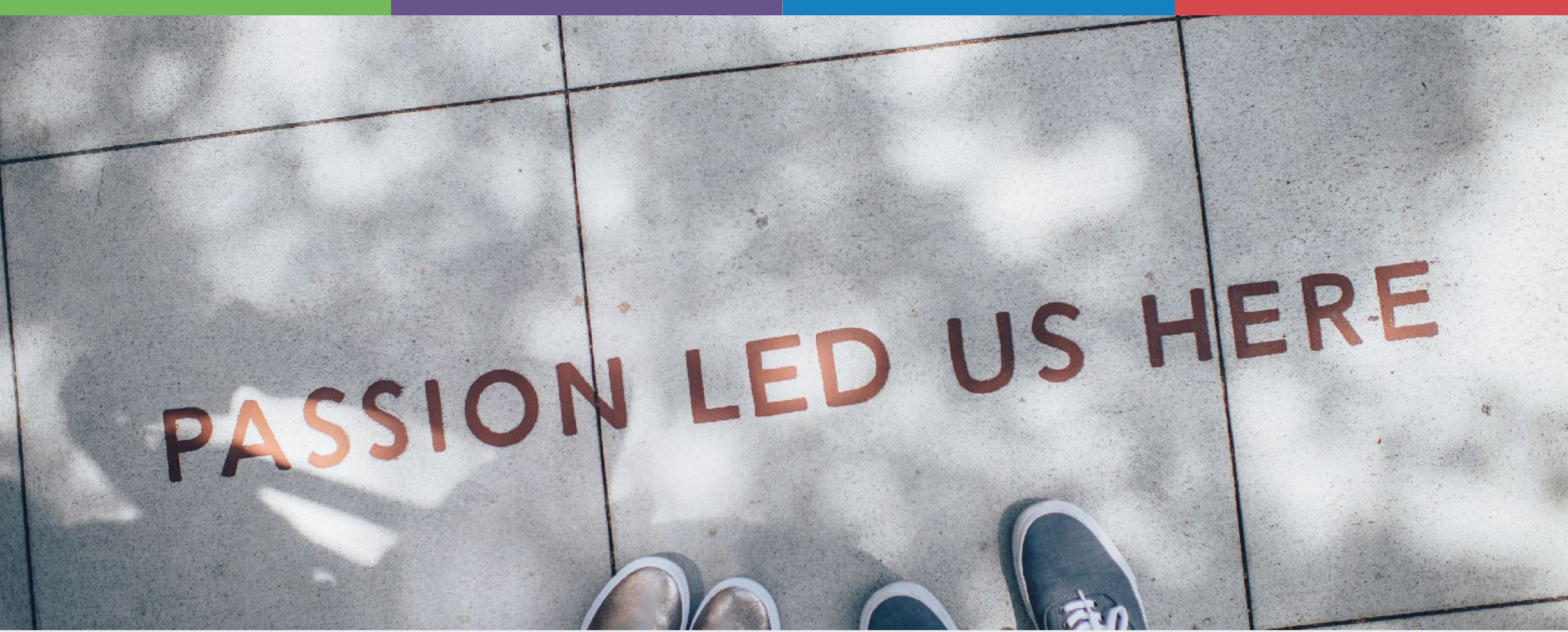
Oct 21

RCE in sensu.instagram.com Reported

Vulnerability with PoC submitted to Facebook's Whitehat program.

Oct 21

RCE in sensu.instagram.com Discovered



How to Roll Out a Bug Bounty Program

Define your Bug Bounty Program

Internal messaging

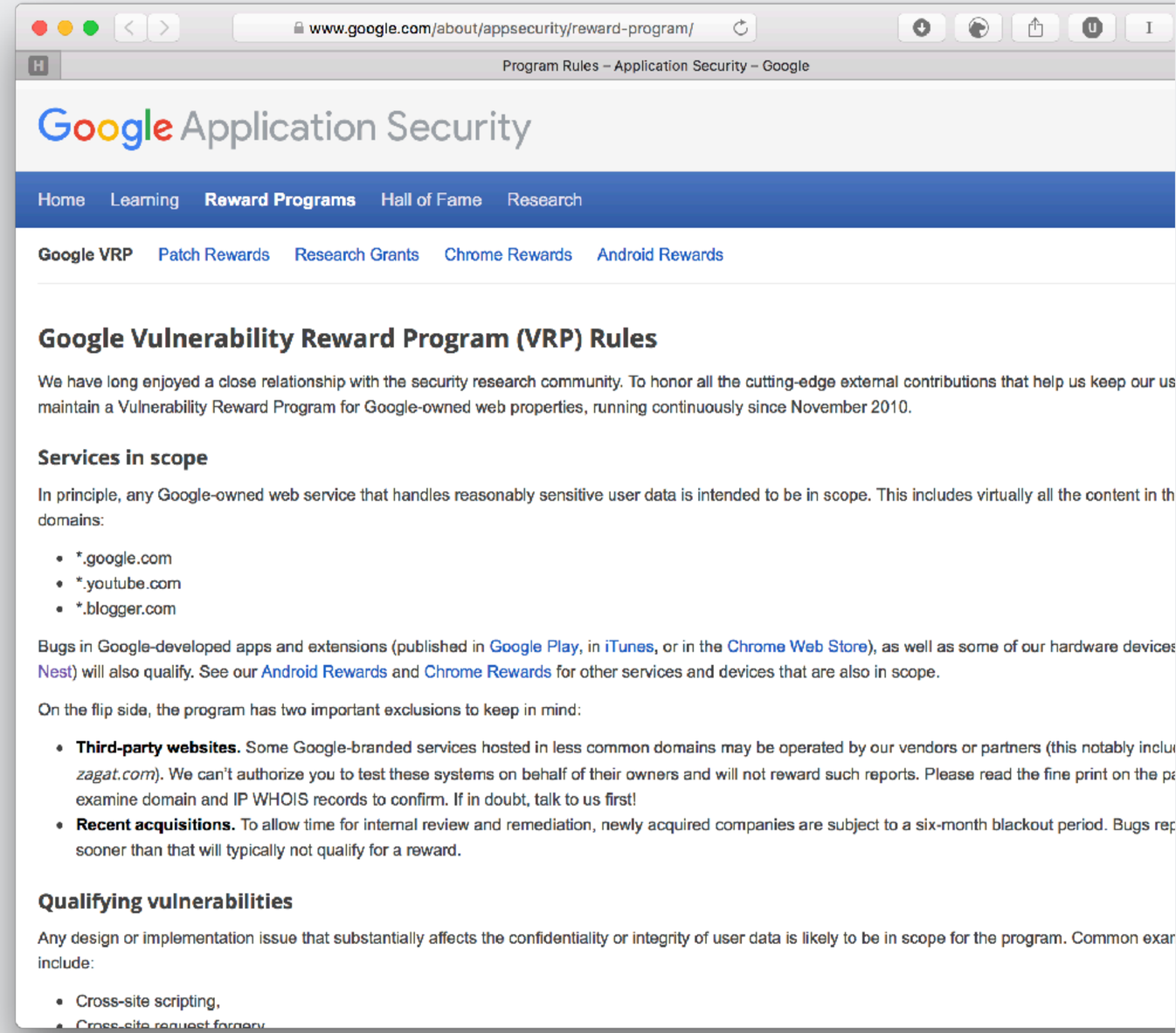
External messaging

Pieces of a Bug Bounty Program

- Public or Private
  - Private (invite only) can be a good first step
- Scope - define this well
- Terms
- Preferred submission process
- Timeline
- Platform

Terms & Conditions

- What is a vulnerability
- How far should the researcher go to prove the issue
- CYA - Legal Team
  - What if the issue is destructive?
  - How much time do you spend trying to reproduce the issue?



The Google VRP is a great example

Let's Talk Rewards

Santiago Lopez @santi_lopezz99 · Apr 18

I'm so happy that i bought my new #Mini #Cooper with the bug bounty money 😌😎.
Thanks again @Hacker0x01, your platform is great 😃#hackerone

Incentives & Rewards

SECURITY INNOVATION

- Swag
- Fame
  - Knuth Reward Check
  - Hall of fame/Leaderboard
- Facebook "Whitehat" debit Card
- Cash rewards $0-$100,000
  - Consider "cool" values ($31337 for top Google Reward)
- Interviews to your security team?

Photo by Mounzer Awad on Unsplash

Preferred Submission Process

SECURITY INNOVATION

Only a recommendation; it’s important to have guidelines

E-mail encryption

- PGP
- SMIME
- Online secure mail

Web Delivery

- Secure dropbox
- Encrypted zip
- Secure collaboration software

Internal Messaging

Let People Know

- Legal Team
  - First contact should not be your legal team
- Marketing
  - How to respond publicly
  - What to say
- Senior Leadership
  - Get buy-in, both for budget and message
- Engineering
  - Set up timelines to respond and fix
- Security Team
  - Get ready to prioritize, respond, and plan

Photo by Jason Rosewell on Unsplash

Make a Plan

SECURITY INNOVATION

- Who is the main point of contact?
- How quickly can you realistically respond?
- How quickly can you realistically remediate?
- What if a critical issue is reported?
- First Contact & Follow up

Photo by Vadim Sherbakov on Unsplash

External Messaging

Website & e-mail

SECURITY INNOVATION

Security Pages

- Disclosure Policy
- Bug Bounty Program
- Mydomain.com/security
- Bug Bounty Hall of Fame

Contact address

- security@
- support@
- bugs@

Social Media

- Announce your bug bounty program
- Reach out to all media platforms, even IRC ->
- Talk about your success
- Blog about announcements & submissions

```
all your base
15:21:39 <@rolle> puistattaa oikein :D
15:21:42 <@mustikkasoppa> rolle luetko :D
15:21:45 <+kOOpa> ite en oo fonttia melkein koskaan säätänyt
15:21:50 <@rolle> soppa joo ku oon kotona
15:21:59 <+kOOpa> jonkun kivan vaan jostain luntannut
15:21:59 <@rolle> kOOpa: saa fonttia säätä, kunhan css:ssä
15:22:15 <@mustikkasoppa> HAA mää tiän miltä haluan otsikon näyttävän :PPP
15:22:21 <@mustikkasoppa> vittu LAG
15:22:40 <@mustikkasoppa> :DDD
15:24:31 <@mustikkasoppa> sain muuten inspan nyt :P
15:24:38 <@mustikkasoppa> \o
15:24:39 <+kOOpa> joo mä meen pelaamaan ->
15:44:23 <@rolle> tein v3:n revolutionary.themestä
15:44:34 <@rolle> http://193.64.18.251/~rolle/revolutionaryv3.theme
15:44:47 <@rolle> tää on kiva
15:44:51 <@rolle> pinkki topicbar<3
15:44:53 <@rolle> sininen aktiivisuus<3
15:45:20 <@Frozenball> pics?
15:45:29 <@mustikkasoppa> :O
15:45:32 <@mustikkasoppa> rolle mulle!
15:45:32 <@mustikkasoppa> :D
15:45:37 <@rolle> mustikkasoppa: ota tuosta :)
15:45:41 <@rolle> http://193.64.18.251/~rolle/revolutionaryv3.theme
15:45:44 <@mustikkasoppa> osaankohan  :DDD
15:45:47 <@mustikkasoppa> yritän
15:46:09 <@rolle> Frozenball: ai haluut nähdä ok
15:46:18 <@rolle> otanpa
15:46:28 <@rolle> sanokaa jotain #soppasella
15:46:33 <@rolle> niin tulee aktiviisuuskin tähän
15:46:40 <@Frozenball> juusto
15:46:41 <@rolle> mustikkasoppa: hailaittaa mua kesämaalla :D
15:46:43 <@Frozenball> aainii
15:46:47 <@rolle> niin tulee hailaitin värikin tähän :D
15:47:02 <@mustikkasoppa> :D
15:47:17 <@mustikkasoppa> ^^
15:47:21 <@mustikkasoppa> teen tota otsikkoa :D
---------------------------------------------------------------------------
 15:48:49 @rolle (+i) Away. 2:#rolleweb (+Cnt)  1:S 5:@#kesäm
#rolleweb>
```

Summary

- Do your research
- Self Assess: are you ready?
- Define your BBP
- Create BBP response team
- Roll out Internal Messaging
- Roll out External Messaging

Joe Basirico
VP of Services
jbasirico@securityinnovation.com
(206) 508-1001