Building a Modern Security Engineering Team

zane@signalsciences.com

@zanelackey

Signal Sciences

Who is this guy anyway?

- Built and led the Etsy Security Team
  - Spoiler alert: what this presentation is about
- Co-founded Signal Sciences

This talk is about lessons learned being at the forefront of the shift to agile/continuous deployment/DevOps

For security teams, the world has changed in fundamental ways:

- Code deployment is now near-instantaneous

For security teams, the world has changed in fundamental ways:

- Code deployment is now near-instantaneous
- Merging of development and operations means more people with production access

For security teams, the world has changed in fundamental ways:

- Code deployment is now near-instantaneous
- Merging of development and operations means more people with production access
- Cost of attack has significantly dropped

Near-instantaneous deployment?

An example: Etsy pushes to production **50 times a day** on average

Constant iteration **in production** via feature flags, ramp ups, A/B testing

But doesn’t the rapid rate of change mean things are less secure?!

Actually, the opposite is true

They key to realize is vulnerabilities occur in **all** development methodologies

They key to realize is vulnerabilities occur in **all** development methodologies

…But there’s no such thing as an out-of-band patch in continuous deployment

Compared to:

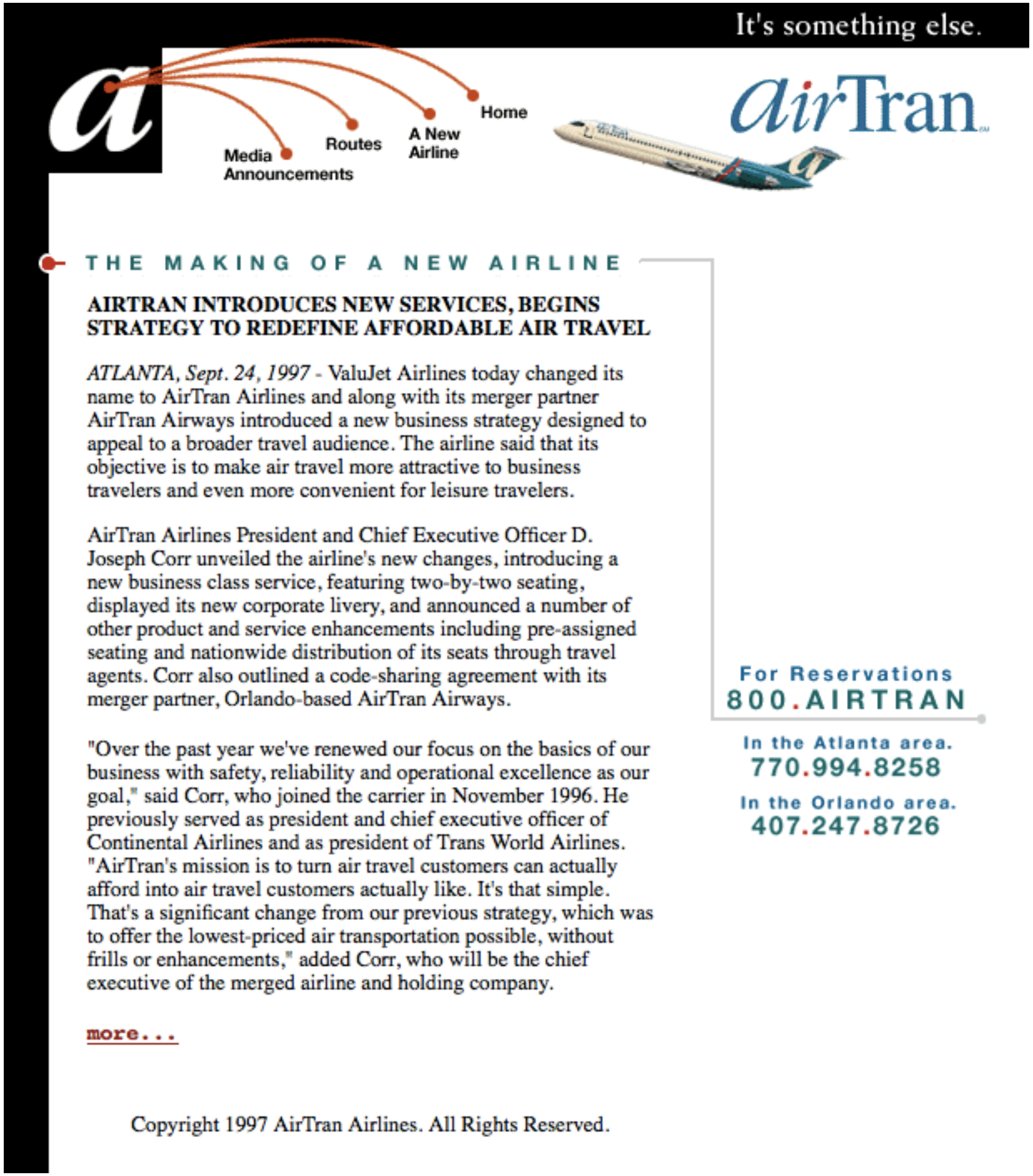
“We’ll rush that security fix. It will go out … in about 6 weeks.”

- **Former** vendor at Etsy

What makes continuous deployment safe?

What makes continuous deployment safe?

Visibility



THE MAKING OF A NEW AIRLINE

AIRTRAN INTRODUCES NEW SERVICES, BEGINS STRATEGY TO REDEFINE AFFORDABLE AIR TRAVEL

ATLANTA, Sept. 24, 1997 - ValuJet Airlines today changed its name to AirTran Airlines and along with its merger partner AirTran Airways introduced a new business strategy designed to appeal to a broader travel audience. The airline said that its objective is to make air travel more attractive to business travelers and even more convenient for leisure travelers.

AirTran Airlines President and Chief Executive Officer D. Joseph Corr unveiled the airline's new changes, introducing a new business class service, featuring two-by-two seating, displayed its new corporate livery, and announced a number of other product and service enhancements including pre-assigned seating and nationwide distribution of its seats through travel agents. Corr also outlined a code-sharing agreement with its merger partner, Orlando-based AirTran Airways.

"Over the past year we've renewed our focus on the basics of our business with safety, reliability and operational excellence as our goal," said Corr, who joined the carrier in November 1996. He previously served as president and chief executive officer of Continental Airlines and as president of Trans World Airlines. "AirTran's mission is to turn air travel customers can actually afford into air travel customers actually like. It's that simple. That's a significant change from our previous strategy, which was to offer the lowest-priced air transportation possible, without frills or enhancements," added Corr, who will be the chief executive of the merged airline and holding company.

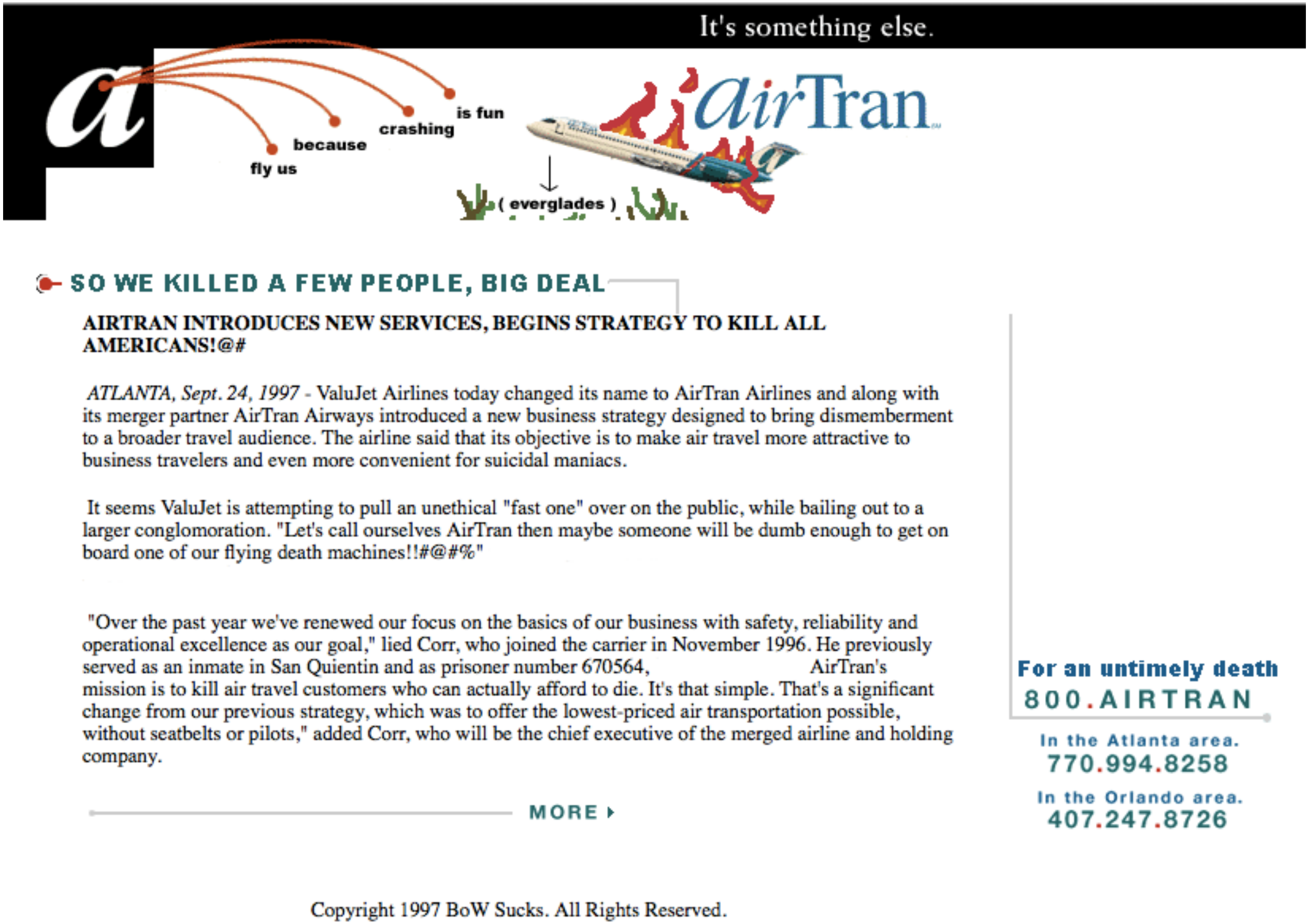
more...

For Reservations
800.AIRTRAN

In the Atlanta area.
770.994.8258

In the Orlando area.
407.247.8726

Copyright 1997 AirTran Airlines. All Rights Reserved.



SO WE KILLED A FEW PEOPLE, BIG DEAL

AIRTRAN INTRODUCES NEW SERVICES, BEGINS STRATEGY TO KILL ALL AMERICANS!@#

ATLANTA, Sept. 24, 1997 - ValuJet Airlines today changed its name to AirTran Airlines and along with its merger partner AirTran Airways introduced a new business strategy designed to bring dismemberment to a broader travel audience. The airline said that its objective is to make air travel more attractive to business travelers and even more convenient for suicidal maniacs.

It seems ValuJet is attempting to pull an unethical "fast one" over on the public, while bailing out to a larger conglomoration. "Let's call ourselves AirTran then maybe someone will be dumb enough to get on board one of our flying death machines!!#@#%"

"Over the past year we've renewed our focus on the basics of our business with safety, reliability and operational excellence as our goal," lied Corr, who joined the carrier in November 1996. He previously served as an inmate in San Quientin and as prisoner number 670564, AirTran's mission is to kill air travel customers who can actually afford to die. It's that simple. That's a significant change from our previous strategy, which was to offer the lowest-priced air transportation possible, without seatbelts or pilots," added Corr, who will be the chief executive of the merged airline and holding company.

MORE ▸

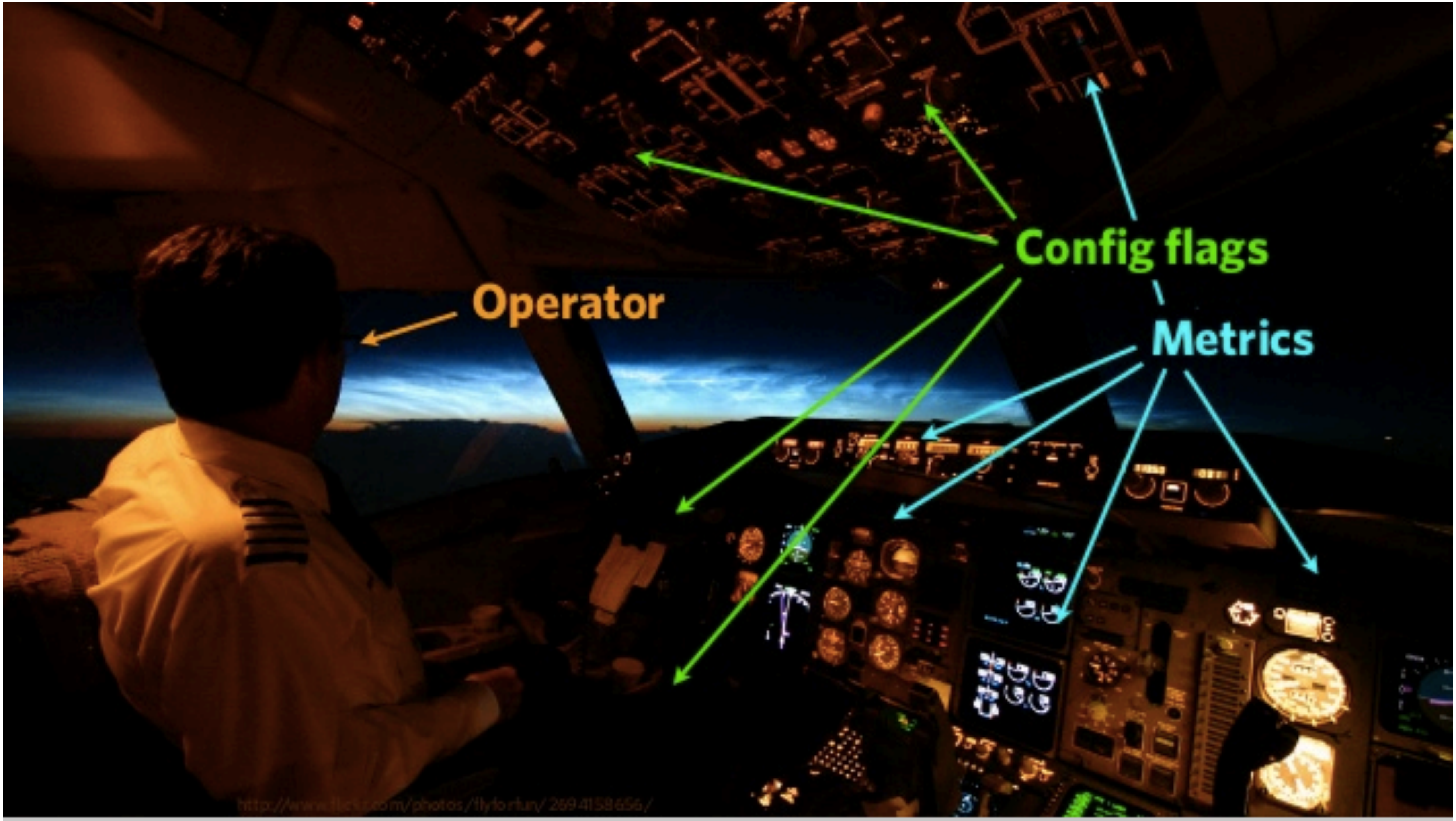
For an untimely death
800.AIRTRAN

In the Atlanta area.
770.994.8258

In the Orlando area.
407.247.8726

Copyright 1997 BoW Sucks. All Rights Reserved.

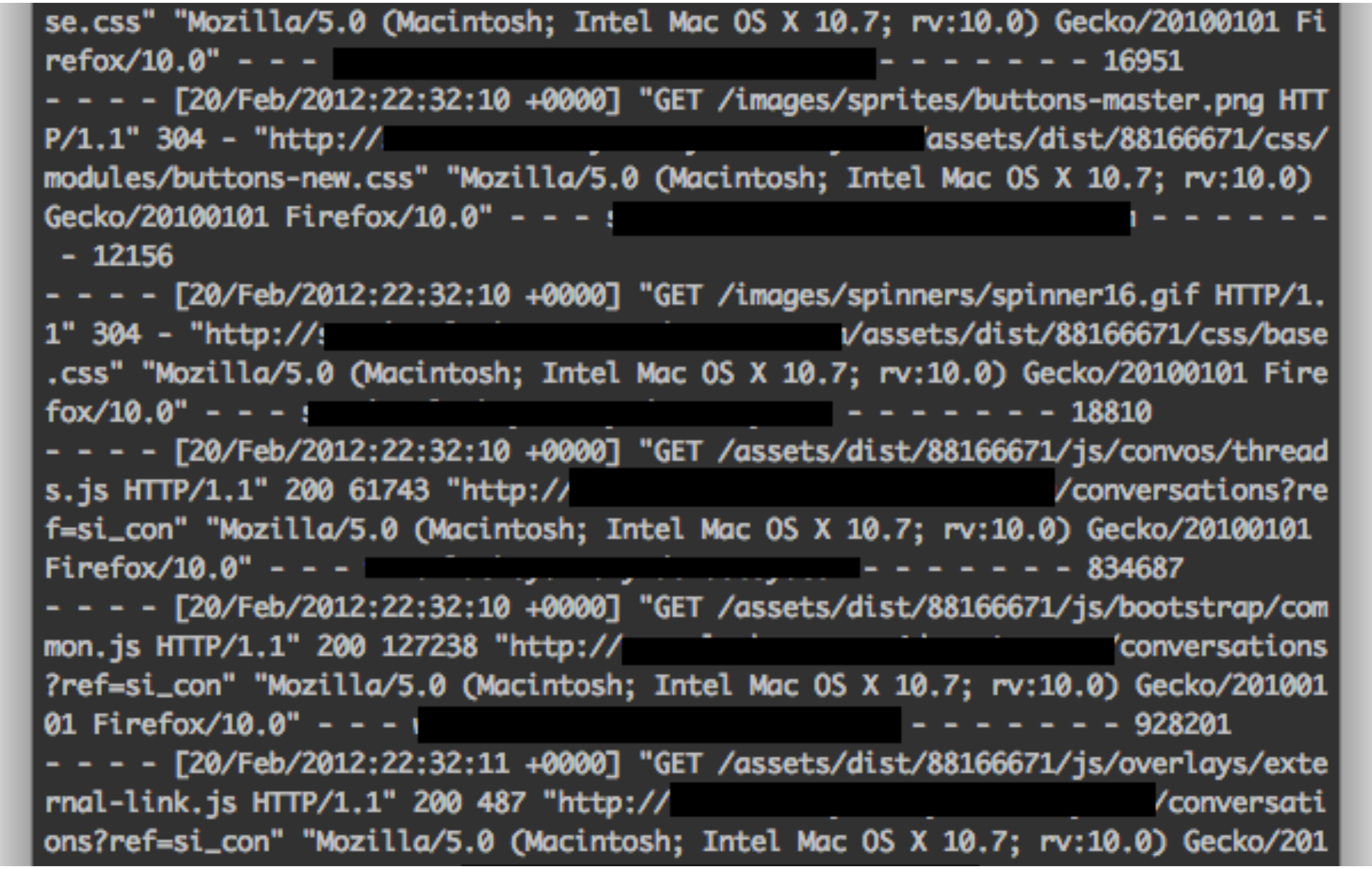
ALL MONITORED HOSTS UP
Thank you for testing.
26.0
13.2
RIPSTOP
DUFFLE



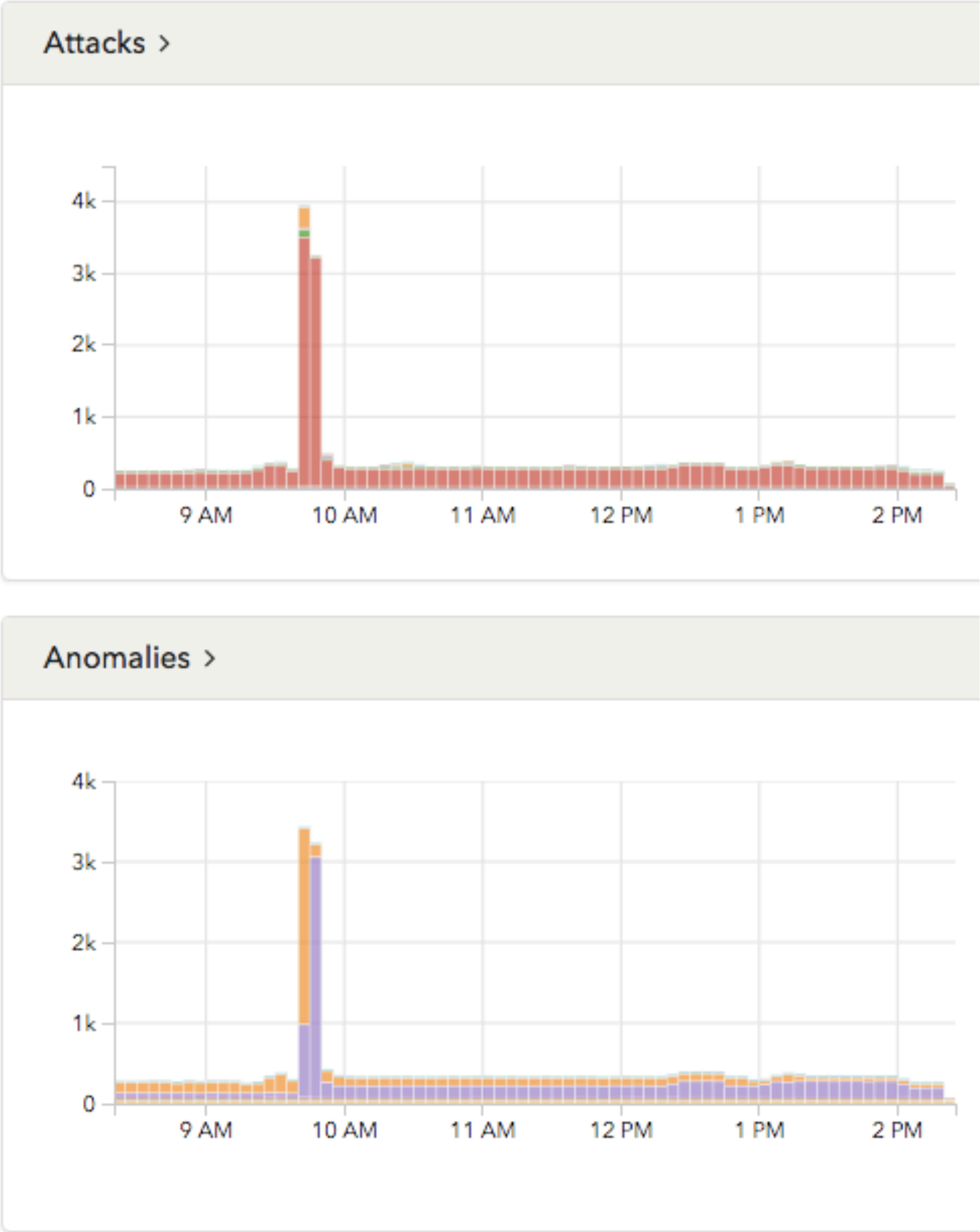
Source: http://www.slideshare.net/mikebrittain/advanced-topics-in-continuous-deployment

The same hard lessons are slowly shifting to security

Ex: Which of these is a quicker way to spot an attack?



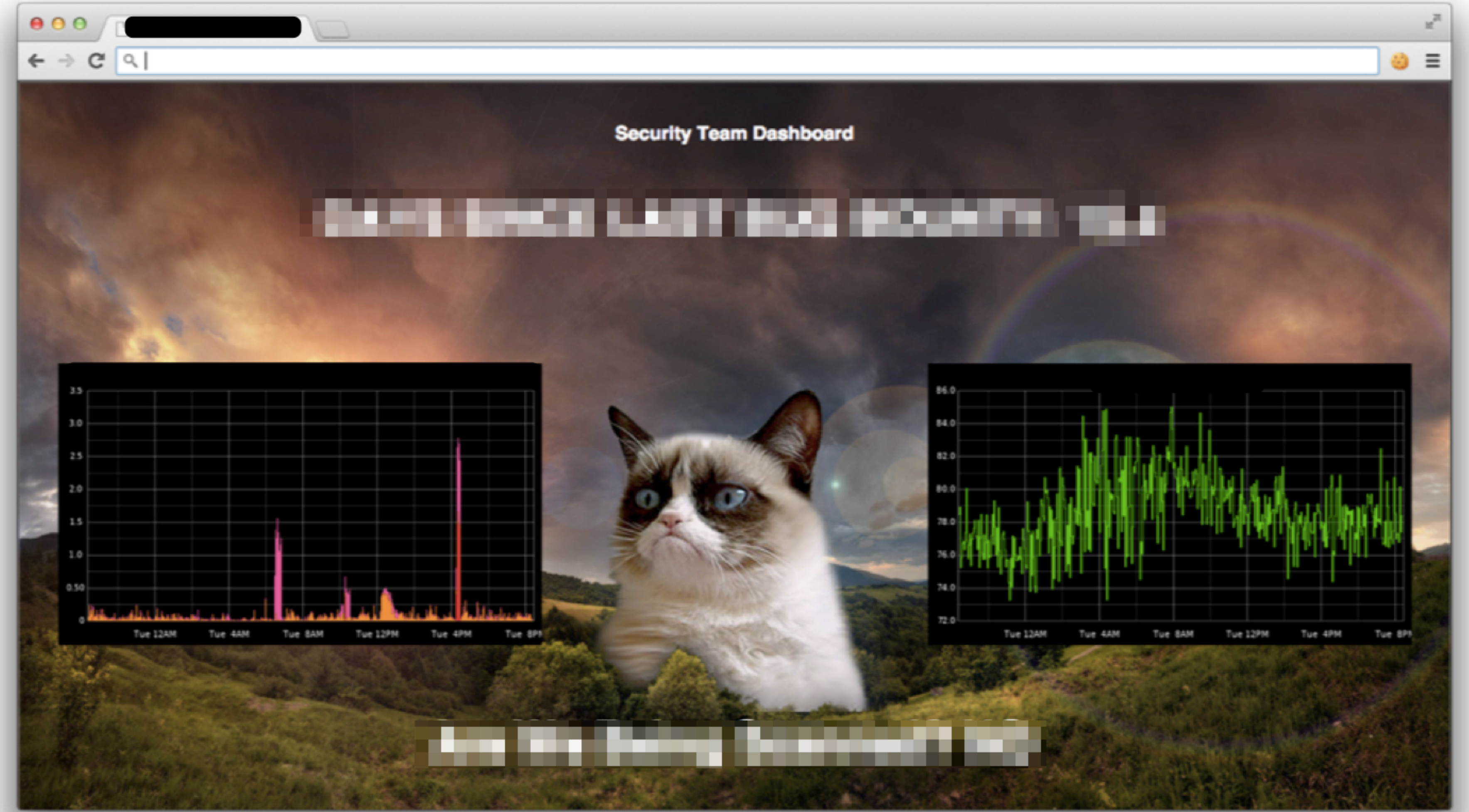
```
se.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/20100101 Fi
refox/10.0" - - - [redacted]- - - - - - - - 16951
- - - - [20/Feb/2012:22:32:10 +0000] "GET /images/sprites/buttons-master.png HTT
P/1.1" 304 - "http://[redacted]assets/dist/88166671/css/
modules/buttons-new.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0)
Gecko/20100101 Firefox/10.0" - - - [redacted] - - - - - - -
 - 12156
- - - - [20/Feb/2012:22:32:10 +0000] "GET /images/spinners/spinner16.gif HTTP/1.
1" 304 - "http://[redacted]/assets/dist/88166671/css/base
.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/20100101 Fire
fox/10.0" - - - [redacted] - - - - - - - - 18810
- - - - [20/Feb/2012:22:32:10 +0000] "GET /assets/dist/88166671/js/convos/thread
s.js HTTP/1.1" 200 61743 "http://[redacted]/conversations?re
f=si_con" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/20100101
Firefox/10.0" - - - [redacted]- - - - - - - - 834687
- - - - [20/Feb/2012:22:32:10 +0000] "GET /assets/dist/88166671/js/bootstrap/com
mon.js HTTP/1.1" 200 127238 "http://[redacted]/conversations
?ref=si_con" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/201001
01 Firefox/10.0" - - - [redacted] - - - - - - - - 928201
- - - - [20/Feb/2012:22:32:11 +0000] "GET /assets/dist/88166671/js/overlays/exte
rnal-link.js HTTP/1.1" 200 487 "http://[redacted]/conversati
ons?ref=si_con" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/201
```



Attacks >

Anomalies >

Surface security info for **everyone**, not just the security team



[redacted]

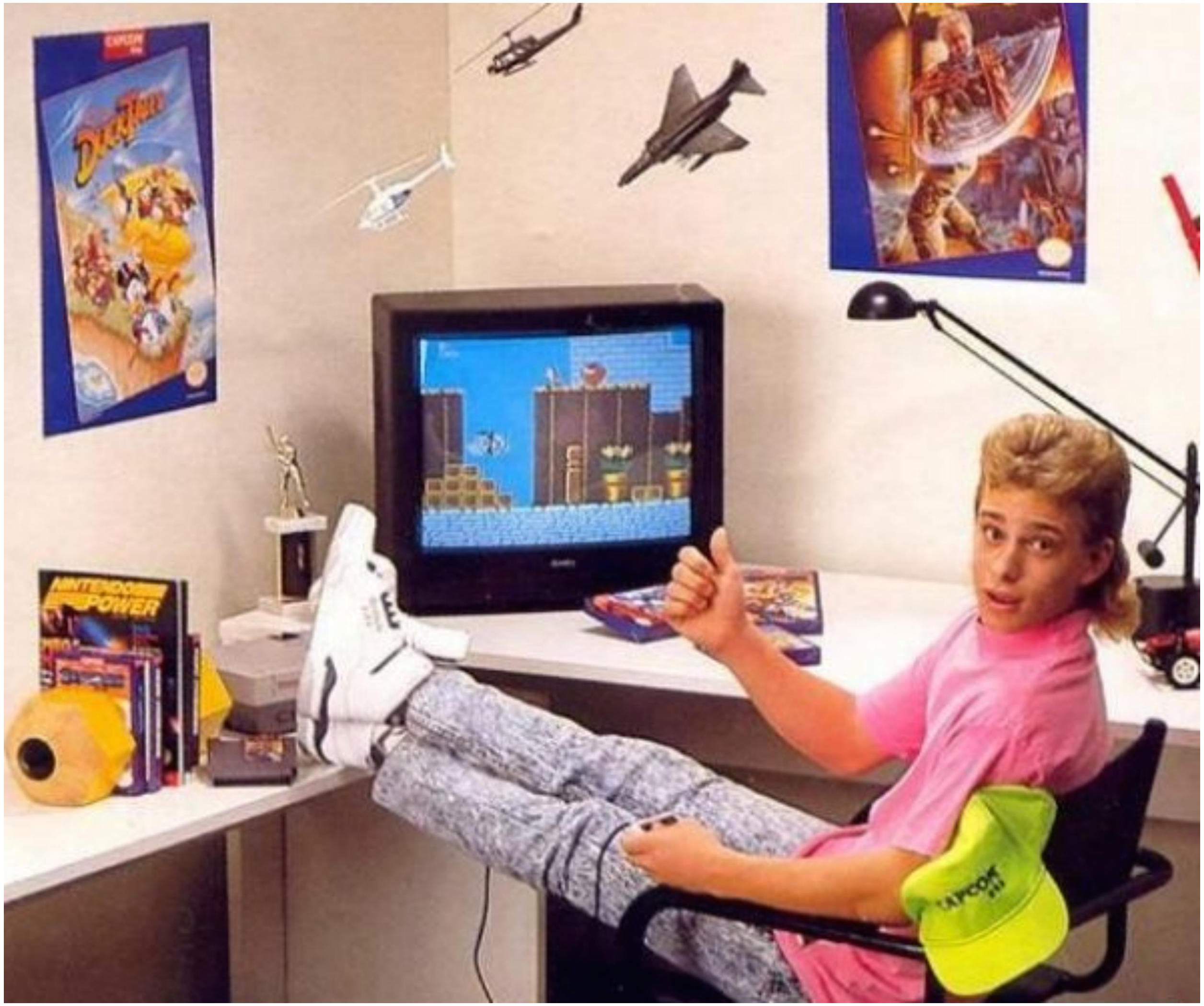
Security Team Dashboard

[redacted]

[redacted]

“Don’t treat security as a binary event”

- @ngalbreath



Building a rad culture

*Mullets sold separately

In the shift to continuous deployment, speed increases by removing organizational blockers

Trying to make security a blocker means you get routed around

Instead, the focus becomes on incentivizing teams to reach out to security

Keys to incentivizing conversation:

- **Don’t be a jerk**. This should be obvious, but empathy needs to be explicitly set as a core part of your teams culture.

Keys to incentivizing conversation:

- **Don’t be a jerk**. This should be obvious, but empathy needs to be explicitly set as a core part of your teams culture.

- **Make realistic tradeoffs**. Don’t fall in to the trap of thinking every issue is critical.
    - Ex: Letting low risk issues ship with a reasonable remediation window buys you credibility for when things actually do need to be addressed immediately.

Keys to incentivizing conversation:

– **Coherently explain impact**. “This would allow all our user data to be compromised if the attacker did X & Y” paints a clear picture, where “The input validation in this function is weak” does not.

Keys to incentivizing conversation:

- **Coherently explain impact**. “This would allow all our user data to be compromised if the attacker did X & Y” paints a clear picture, where “The input validation in this function is weak” does not.
- **Reward communication with security team**. T-Shirts, gift cards, and high fives all work (shockingly) well.

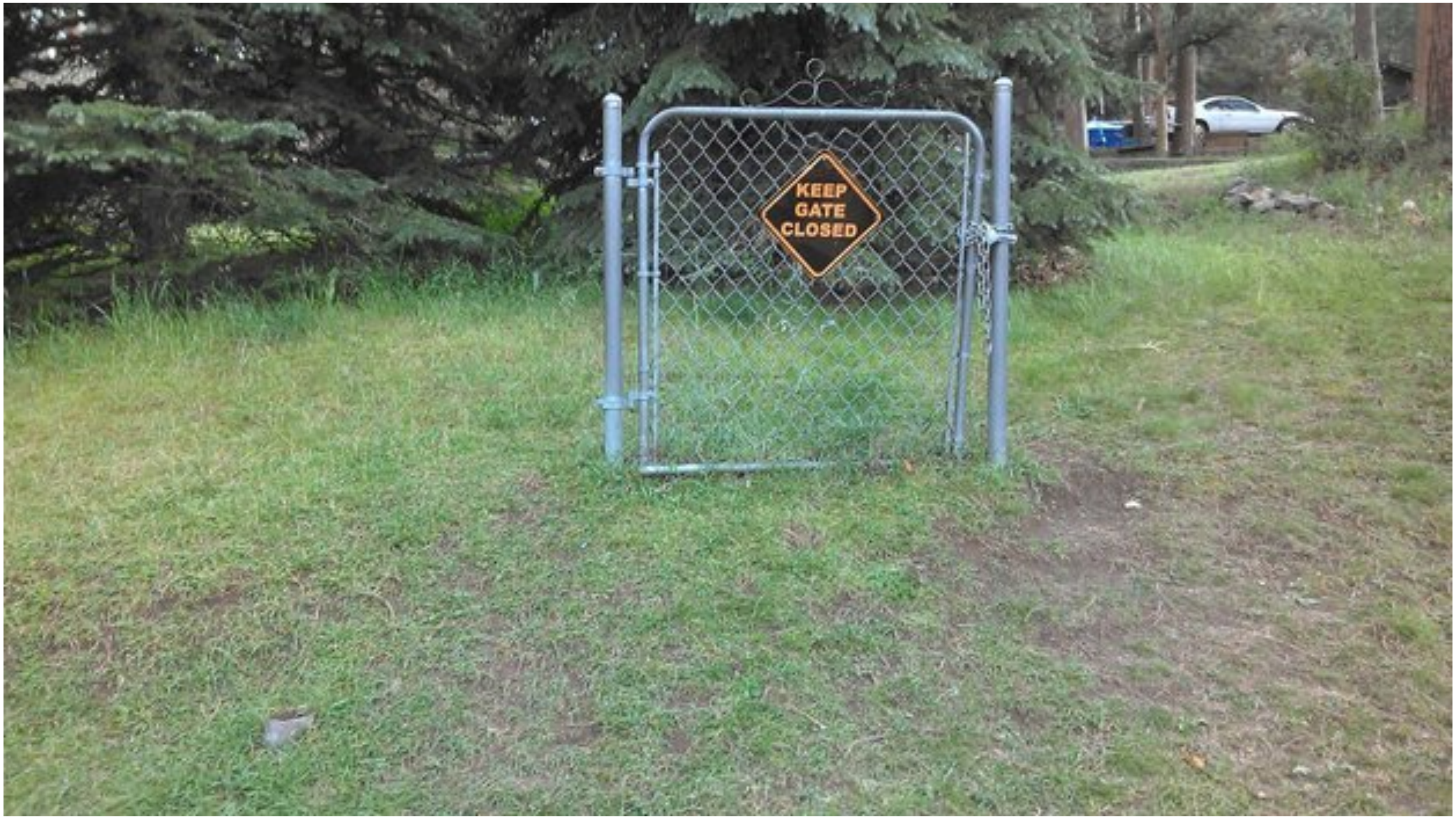
Keys to incentivizing conversation:

- **Take the false positive hit yourself**. Don’t send unverified issues to dev and ops teams. When issues come in, have the secteam verify and make first attempt at patch.

Keys to incentivizing conversation:

- **Take the false positive hit yourself**. Don't send unverified issues to dev and ops teams. When issues come in, have the secteam verify and make first attempt at patch.

- **Scale via team leads**. Build relationships with technical leads from other teams so they make security part of their teams culture.



Access restrictions

Startups begin with a simple access control policy: Everyone can access everything

As organization grow there will be more pressure to institute access policies

The key to remember is **don’t take away capabilities**

Methodology:

1. Figure out what capability is needed

Methodology:

1. Figure out what capability is needed

2. Build an alternate way to perform the needed function in a safe way

Methodology:

1. Figure out what capability is needed

2. Build an alternate way to perform the needed function in a safe way

3. Transition the organization over to the safe way

Methodology:

1. Figure out what capability is needed

2. Build an alternate way to perform the needed function in a safe way

3. Transition the organization over to the safe way

4. Alert on any usage of the old unsafe way

EX: SSH access to production systems

Security policy goal: Eliminate unneeded access to production systems

  - Why do developers do it? Ex: To view error logs

Security policy goal: Eliminate unneeded access to production systems

- Why do developers do it? Ex: To view error logs
- Build alternate approach: Send the logs to central logging service (ex: logstash, splunk, etc)

Security policy goal: Eliminate unneeded access to production systems

- Why do developers do it? Ex: To view error logs
- Build alternate approach: Send the logs to central logging service (ex: logstash, splunk, etc)
- Publicize the new tooling to the organization

Security policy goal: Eliminate unneeded access to production systems

- Why do developers do it? Ex: To view error logs
- Build alternate approach: Send the logs to central logging service (ex: logstash, splunk, etc)
- Publicize the new tooling to the organization
- After majority of transition, alert on any logins to production systems by non-sysops

Increasing attacker cost

Bug bounties/disclosure programs are tremendously useful. If you're not working towards launching one, strongly consider it.

Common concerns about launching a bounty:

1. **Budgetary concerns**.

1. **Risk of inviting attacks**.

Common concerns about launching a bounty:

1. **Budgetary concerns**. Money is rarely the main motivation for participants, you can launch a bounty with just a hall of fame and still get great submissions.

1. **Risk of inviting attacks**.

Common concerns about launching a bounty:

1. **Budgetary concerns**. Money is rarely the main motivation for participants, you can launch a bounty with just a hall of fame and still get great submissions.

1. **Risk of inviting attacks**. It’s the Internet. You’re already getting pentested continuously, you’re just not receiving the report.

The ultimate goals of a bug bounty are threefold:

1. Incentivize people to report issues to you in the first place

The ultimate goals of a bug bounty are threefold:

1. Incentivize people to report issues to you in the first place

2. Drive up cost of vulnerability discovery and exploitation for attackers

The ultimate goals of a bug bounty are threefold:

1. Incentivize people to report issues to you in the first place

2. Drive up cost of vulnerability discovery and exploitation for attackers

3. Provide an external validation of where your security program is working (and where it's not)

Before you launch, record what vulnerability classes you expect to see and what you don’t.

Before you launch, record what vulnerability classes you expect to see and what you don’t.

Compare this against the issues actually reported.

Keep metrics on:

- Number of bugs reported and severities

- Time to remediation of reported issues

You want both of these metrics to **trend down** over time

Practical considerations:

- Inform **all teams** before bounty launch, especially non-engineering teams
  - Ex: Customer Support

Practical considerations:

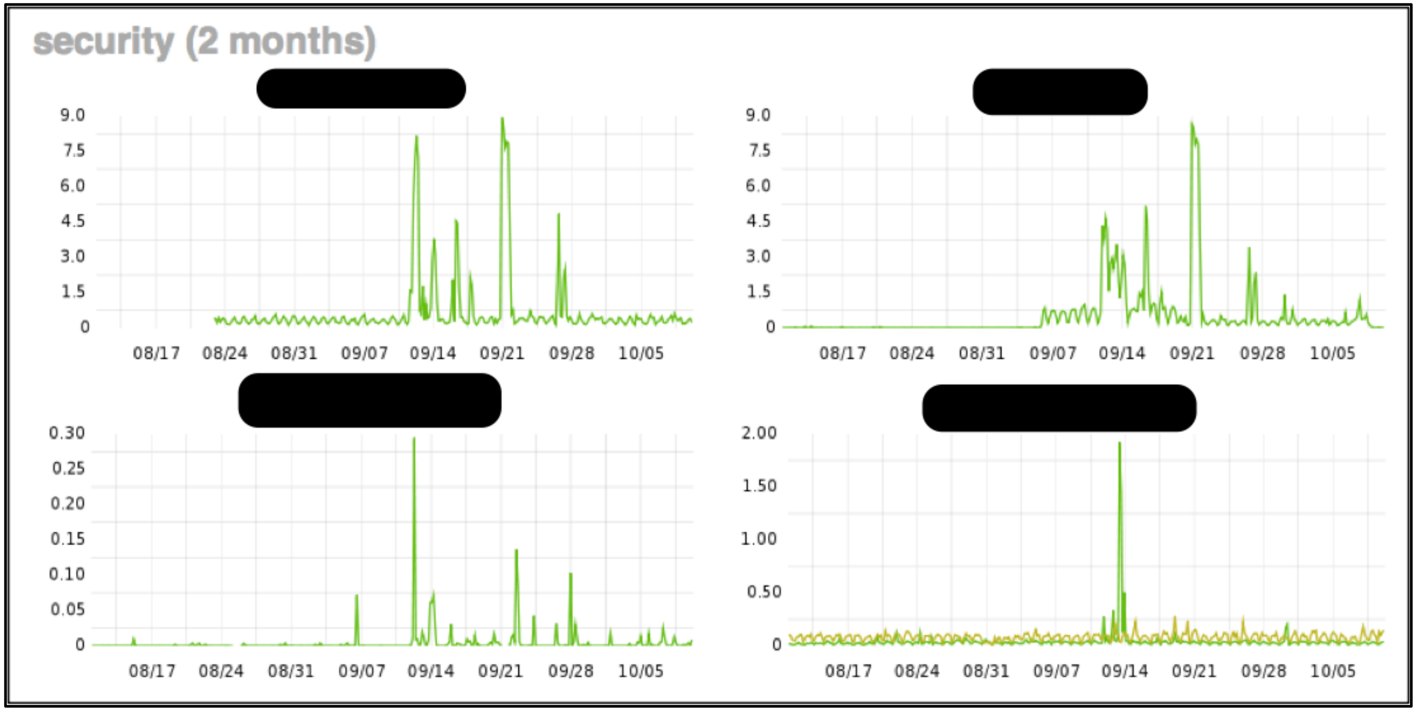
- Inform **all teams** before bounty launch, especially non-engineering teams
  - Ex: Customer Support

- Attacks will start almost immediately

For Etsy bug bounty launch, time from announcement to first attack: **13min**

Practical considerations:

- Your first **2-3 weeks** will be intense. Have as many people as you can dedicated to triage and response



Practical considerations:

- Operationally review any helper systems for scaling problems beforehand
  - When 10-100x traffic hits helper systems your security team uses, what falls over?

Practical considerations:

- Operationally review any helper systems for scaling problems beforehand
  - When 10-100x traffic hits helper systems your security team uses, what falls over?

- Money is almost never the main motivation for bounty participants, hall of fame credit is

Practical considerations:

- Operationally review any helper systems for scaling problems beforehand.
  - When 10-100x traffic hits helper systems your security team uses, what falls over?

- Money is almost never the main motivation for bounty participants, hall of fame credit is

- Key to great researcher interaction is frequent and transparent communication

TL;DR

(The section formerly known as “Conclusions”)

- Adapt security team culture to DevOps and continuous deployment by:
  - Surfacing security monitoring and metrics
  - Incentivize discussions with the security team
  - When creating policy, don’t take away capabilities

- Drive up attacker cost through bug bounty programs, countering phishing, and running realistic attack simulations

Thanks!

zane@signalsciences.com @zanelackey