

# Lessons Learned Embracing DevOps + Security

[zane@signalsciences.com](mailto:zane@signalsciences.com)

@zanelackey



# Who you'll be heckling today

- Started out in pentesting
  - iSEC Partners / NCC Group
- Moved to defense
  - First head of security at Etsy, built and lead the security group
- Now Co-Founder / CSO at Signal Sciences
  - Delivering a NGWAF and RASP to defend web applications / APIs / microservices

# So what is this talk about anyway?

Lessons learned being at the forefront of  
the shift to DevOps/Cloud

Spoiler: Security shifts from being a gatekeeper to enabling teams to be secure by default

What has changed?

# The new realities in a DevSecOps world:

1. Changes happen multiple orders of magnitude faster than previously
  - Deployments go from a few a year to a few a week, month, or even day
  - Many injection points for security drops to few injections point
3. Decentralized ownership of deployment:
  - The long and perilous journey of *Dev->QA->Security->Dev->Sysops->Production* becomes just *Dev->Production*
  - As Dev/DevOps teams own their own ability to build and deploy production infrastructure/apps, conversations with security become opt-in rather than mandated
    - A large culture shift is necessary around this
      - » Spoken previously on this:  
<http://www.slideshare.net/zanelackey/building-a-modern-security-engineering-organization>

# The new realities in a DevSecOps world:

- Security can no longer be “outsourced” to the security team, but rather that the security team’s mission changes to providing the resources for teams to be **security self-sufficient**
- Security only becomes successful if it can bake in to the Development/DevOps process



Let's change our approach



What new concepts should security focus on?

What new concepts should security focus on?

**Visibility + Feedback**

Except... These aren't new concepts!

Performance monitoring, data analytics,  
A/B testing are all about visibility +  
feedback

The same hard lessons are slowly shifting  
to security

First, a story from the old days...

It's something else.



Media  
Announcements

Routes

A New  
Airline

Home



AirTran™

## 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**

It's something else.



## 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 conglomeration. "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 Quentin 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**

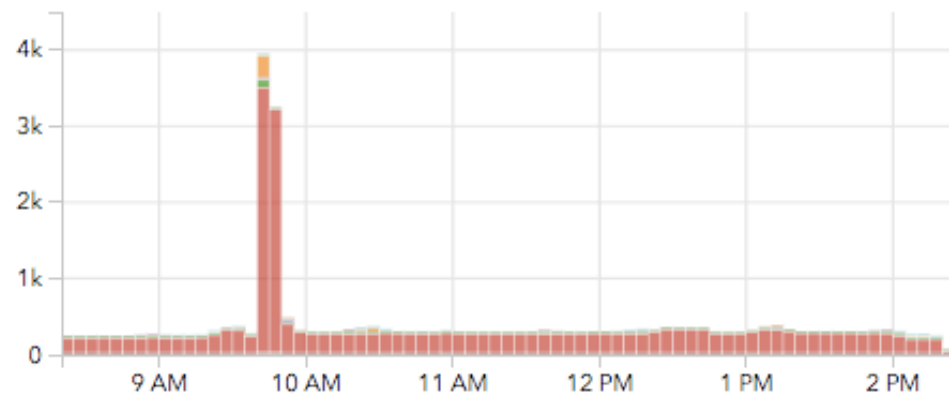


How can we improve?

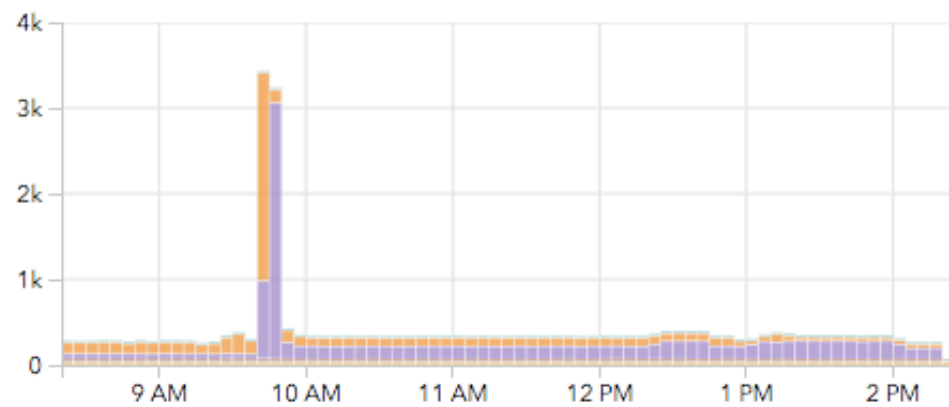
Ex: Which of these is a quicker way to spot an attack?

```
se.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/20100101 Firefox/10.0" - - - - - 16951
- - - - [20/Feb/2012:22:32:10 +0000] "GET /images/sprites/buttons-master.png HTTP/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" - - - - - 12156
- - - - [20/Feb/2012:22:32:10 +0000] "GET /images/spinners/spinner16.gif HTTP/1.1" 304 - "http://[REDACTED]v/assets/dist/88166671/css/base.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/20100101 Firefox/10.0" - - - - - 18810
- - - - [20/Feb/2012:22:32:10 +0000] "GET /assets/dist/88166671/js/convos/threads.js HTTP/1.1" 200 61743 "http://[REDACTED]/conversations?ref=si_con" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/20100101 Firefox/10.0" - - - - - 834687
- - - - [20/Feb/2012:22:32:10 +0000] "GET /assets/dist/88166671/js/bootstrap/common.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/20100101 Firefox/10.0" - - - - - 928201
- - - - [20/Feb/2012:22:32:11 +0000] "GET /assets/dist/88166671/js/overlays/external-link.js HTTP/1.1" 200 487 "http://[REDACTED]conversations?ref=si_con" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0) Gecko/201
```

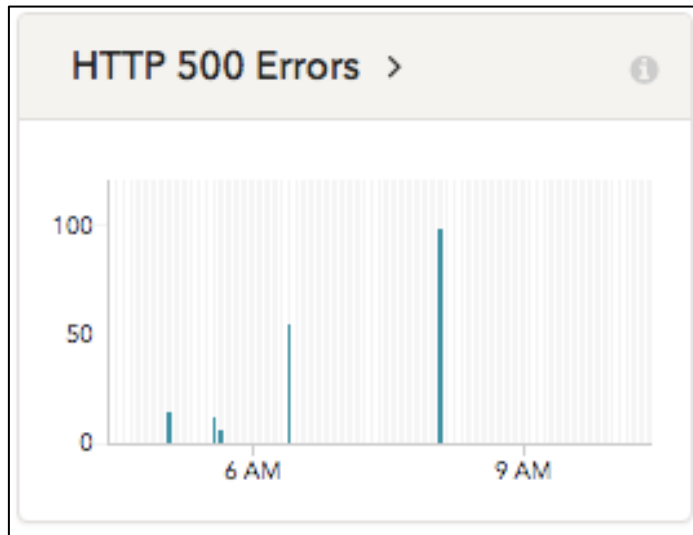
## Attacks >



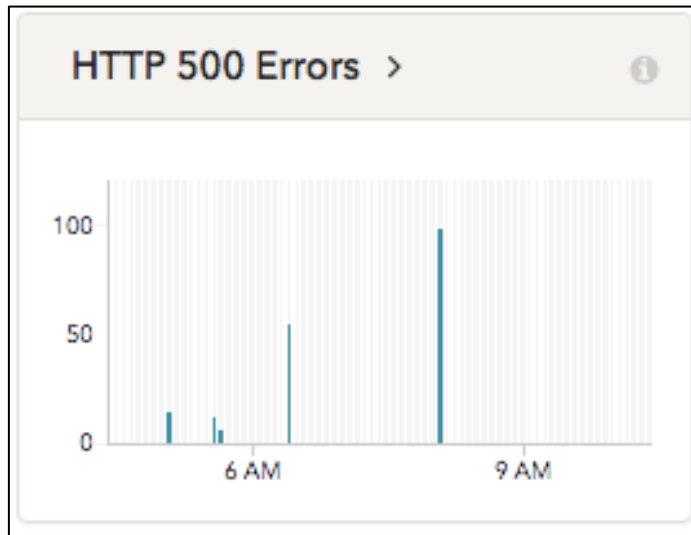
## Anomalies >



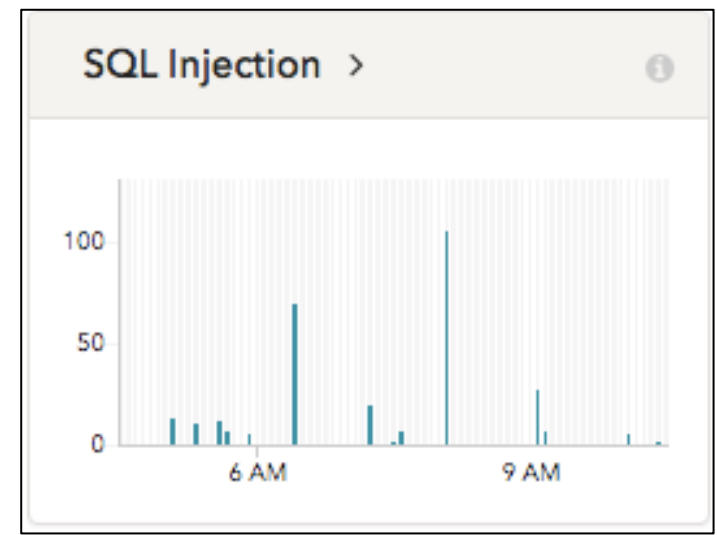
Surface security visibility for **everyone**, not  
just the security team  
(if the security team even exists)



This graph provokes wildly different assumptions from Development, DevOps, and Security teams



+



Context is key, for *\*all\** groups



Obtaining better feedback



Take the lessons of DevOps game days  
and apply them to security

# Three keys to modern feedback loops:

1. Combination of bug bounty + pentests

# Three keys to modern feedback loops:

1. Combination of bug bounty + pentests
2. Bounty is not a replacement for pentest, it augments pentest

# Three keys to modern feedback loops:

1. Combination of bug bounty + pentests
2. Bounty is not a replacement for pentest, it augments pentest
3. Bounty gives general but more real time feedback, pentest shifts to giving more directed but less frequent feedback

# Visibility + Feedback success story:

“I discovered the vulnerability late Friday afternoon and wasn't quite ready to email it to them ... [Etsy] had **detected my requests and pushed a patch** Saturday morning **before I could email them**. This was by far the fastest response time by any company I've reported to.”

- Source: [https://www.reddit.com/r/netsec/comments/vbrzg/etsy\\_has\\_been\\_one\\_of\\_the\\_best\\_companies\\_ive](https://www.reddit.com/r/netsec/comments/vbrzg/etsy_has_been_one_of_the_best_companies_ive)

Every dev methodology has vulnerabilities, but the ability to **react quickly** is what makes DevOps a net positive for security

...but only if we have something to react to

So embrace DevOps, Cloud, and other means of increasing velocity safely by obtaining:

**Visibility + Feedback**



# Thanks!



[zane@signalsciences.com](mailto:zane@signalsciences.com)

@zanelackey