August 2017

August 15, 2017

SANS

Continuous Opportunity: DevOps & Security

SANS AppSec
APPLICATION & SOFTWARE SECURITY

C U R R I C U L U M

Get the right training to build secure applications.

PLATFORM SECURITY

DEV531
Defending Mobile Applications Security Essentials

DEV541
Secure Coding in Java/JEE
GSSP-JAVA

DEV544
Secure Coding in .NET
GSSP-NET

CORE

STH.DEVELOPER
Application Security Awareness Modules

DEV522
Defending Web Applications Security Essentials
GWEB

DEV534
Secure DevOps: A Practical Introduction

SEC540
Secure DevOps and Cloud Application Security

SPECIALIZATION

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing and Ethical Hacking

ASSESSMENT

AppSec CyberTalent Assessment
sans.org/appsec-assessment

@sansappsec

software-security.sans.org

Introduction

Ben Allen

- Security Engineer at SANS Institute
- Operations Engineer, Developer at SANS prior to Security
- Network Security Analyst … Architect at UMN
- GCIA, GPEN, GWEB, GWAPT, GMON

- Contact information

ben.allen@mrsecure.org @mr_secure

Agenda

- Continuous Opportunity: DevOps & Security

CONTINUOUS OPPORTUNITY

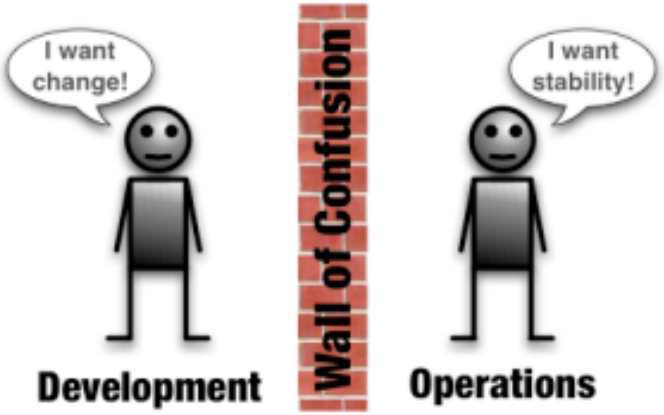
1. *The DevOps Movement*
2. **Shifting Security Left**
3. **Examples**

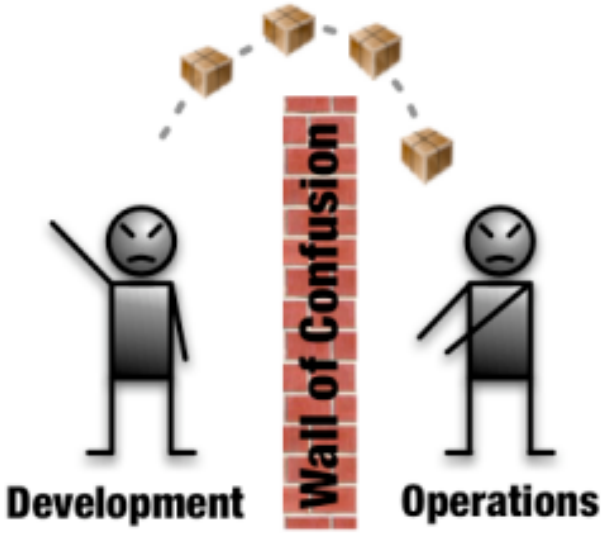
A LONG TIME AGO IN A GALAXY FAR, FAR AWAY

- Waterfall development
  - Phased delivery in large projects
- Slow, gated deployment cycles
  - Several months between releases
- Numerous handoffs between teams
  - Dev -> QA -> Users -> Ops -> Sec

HOW'S THAT WORKING FOR YOU?

- Customers provide feedback too late in the process
- Delays between handoffs
- Security is left until the very end
- High risk / failed deployments
- Slow deployment cycles cause:
  - Projects are delayed and over budget
  - Long zero-day vulnerability windows





HOW'S THAT WORKING FOR YOU?

BREAKING DOWN THE WALLS

- Agile
  - Break down walls between development and the business / customer
- DevOps
  - Break down walls between development and operations
- SecDevOps
  - Break down walls between security and development, operations, business

DEVOPS UNICORNS

Much of the Security DNA in DevOps comes from a few leaders aka “unicorns”:

- Etsy
  - Security in continuous delivery, “a Just Culture”
- Netflix
  - Security in AWS, Simian Army
- Facebook
  - Security at scale, OSQuery
- Twitter
  - Self-service security for developers

CASE STUDY | ETSY BEFORE

Online crafts market place (PCI regulated), established in 2005. Over 1 million sellers, 21 million buyers.

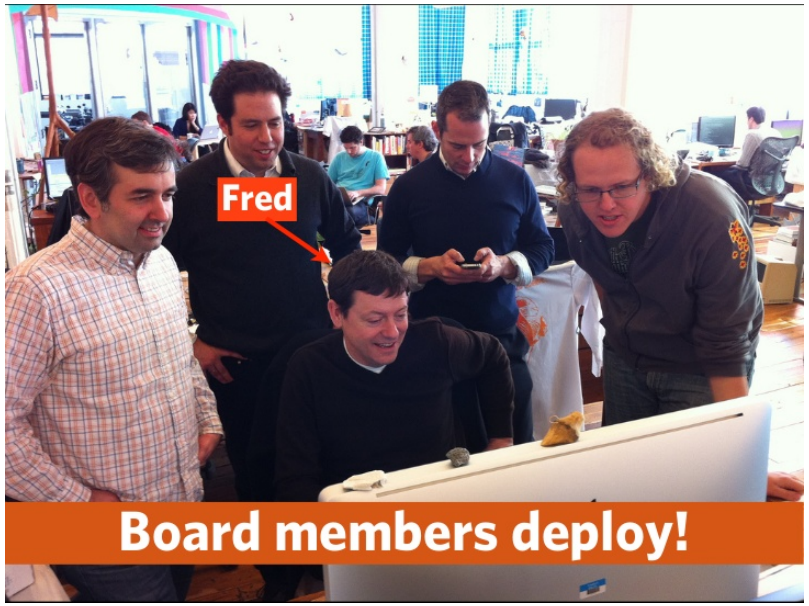
In the beginning (2008):

- Difficulty scaling up engineering, ops teams
- Reliability, downtime problems during deployments
- Production releases 2 times per week
- Each release takes 4 hours
- Deployment process of a large enterprise

CASE STUDY | ETSY AFTER

Fast forward to 2012:

- Continuous Deployment (CD)
  - 50 changes to production per day
- Dark launching (aka feature flags)
- A Just Culture
  - Blameless post-mortems (and Morgue)
  - It is safe to make mistakes – as long as you participate in solving them
  - Record what happened and learn from it
- Dev and Ops all take on-call rotations
- Measure and track everything



DEVOPS PRINCIPLES

DevOps is about CAMS:

- **Culture** - People and process first. If you don't have culture, all automation attempts will be fruitless.
- **Automation** - This is where you start once you understand your culture. At this point, the tools can start to stitch together an automation fabric for DevOps.
- **Measurement** - If you can't measure, you can't improve.
- **Sharing** - Sharing is the feedback loop in the CAMS cycle.

CHEF™

John Willis

What Devops Means to Me, July 2010

WHY? - DEVOPS RESULTS

This faster delivery cycle lets teams experiment, creating a feedback loop with customers. The result? The entire organization benefits, as measured by profitability, productivity, and market share.

2017 State of DevOps Report

2017 STATE OF DEVOPS

Puppet / DORA 2017 State of DevOps Report for high-performing organizations:

- Deploy changes 46 times more often
- Lead times are >440 times shorter
- Change failure rate is 5 times lower
- Failure recovery is 96 times faster
- Spend 50% less time remediating security issues

- https://puppet.com/2017-devops-report

Agenda

- Continuous Opportunity: DevOps & Security

CONTINUOUS OPPORTUNITY

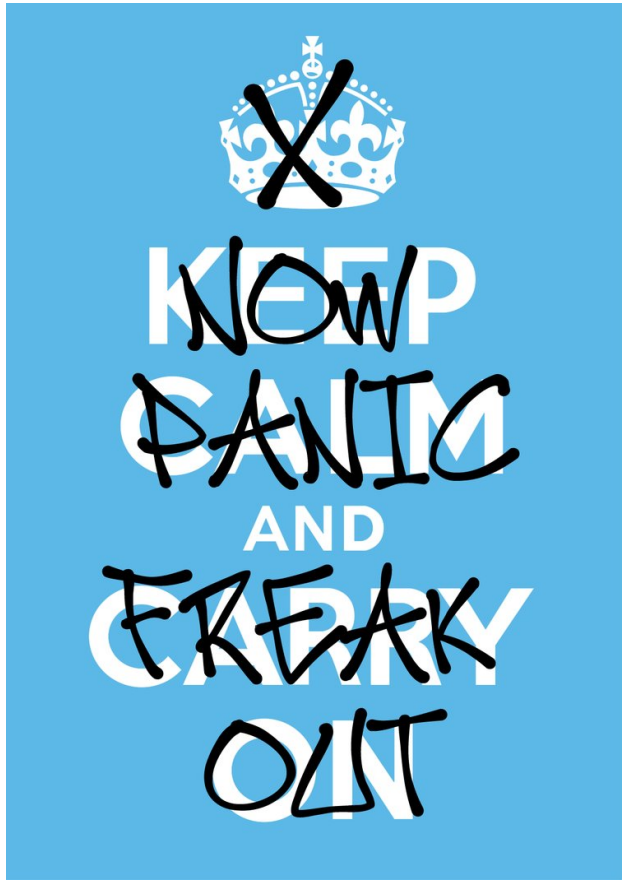
1. **The DevOps Movement**
2. ***Shifting Security Left***
3. **Examples**

50 DEPLOYMENTS A DAY!

How does security keep up?

No pen testing?

No control gates?

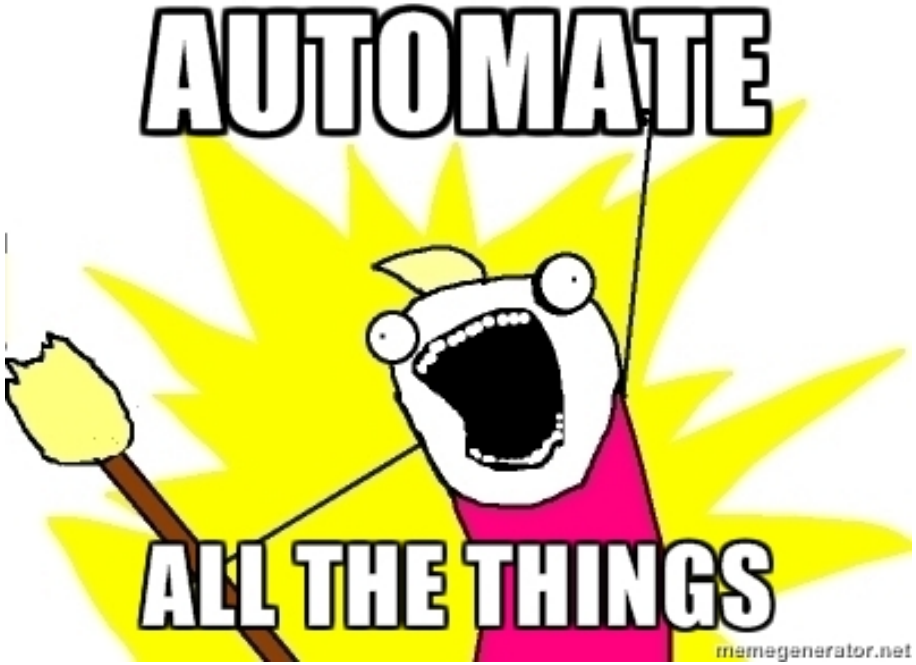


No time for source code assessments?

No security sprints?

CAMS - AUTOMATION

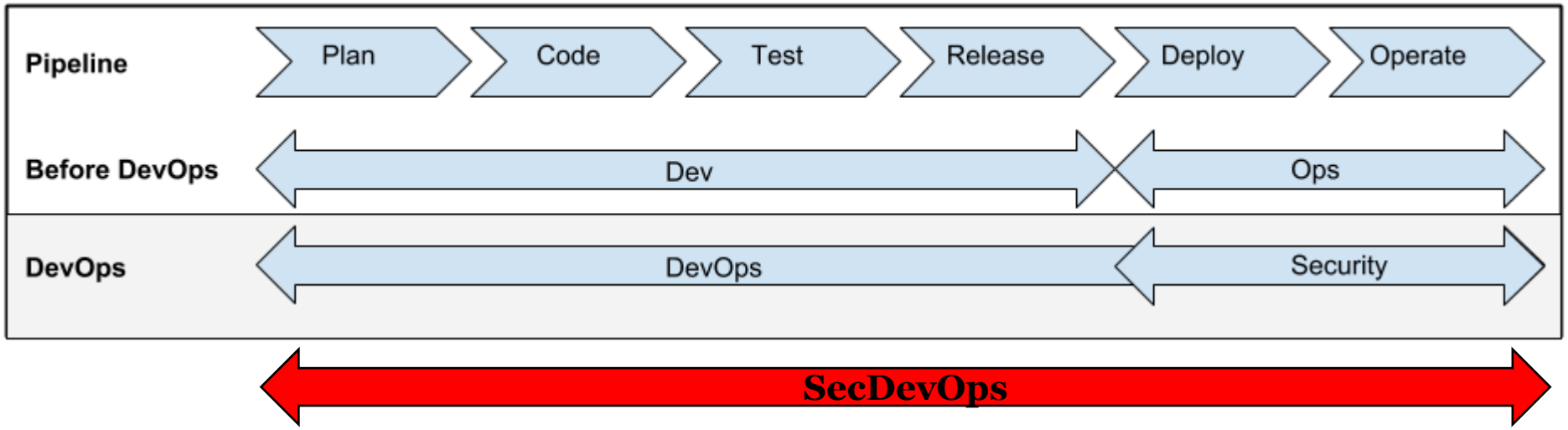
- Configuration Management
  - aka Infrastructure as Code
  - Puppet, Chef, Ansible, Salt, CFEngine
- Continuous Integration
  - Jenkins, Travis, Bamboo, TeamCity
- Continuous Delivery
  - Jenkins, Chef Delivery, Atlassian Bamboo, Amazon AWS Code Pipeline
- Continuous Deployment
- Continuous Monitoring



SHIFTING SECURITY LEFT

Keep up with the pace of continuous delivery by:

- Identify risks using threat modeling during planning
- Automate unit testing for security stories
- Iterative, incremental scans during code, test, and release



CAST STUDY | ETSY'S SECURITY PROGRAM | STEP 1 - 3

1. Don't be an InfoSec jerk. Build security into the frameworks.
2. If it moves, graph it! Real-time monitoring for building attack-driven security defenses
3. Just ship it! Every engineer can push to prod at any time, **including security**

CAST STUDY | ETSY'S SECURITY PROGRAM | STEP 4 - 7

4 Security cannot be a blocker. Don't cry wolf. Practical, realistic trade-offs.

5 Designated hackers assigned to a handful (~ 5) projects.

6 Engineering / Security job rotations

7 Bug bounties, both internal and external

SHIFTING SECURITY LEFT – CONTINUOUS INTEGRATION

Make security a first class citizen during development workflow:

- Static Application Security Testing (SAST) is built into the IDE
- Commits trigger automated security scans (out of band)
- Light-weight, **accurate** static analysis scans (in the pipeline)
- Alerts when high-risk code is changed
- Automated unit testing for security features
- Fast accurate feedback which returns pass / fail results

STATIC ANALYSIS TOOLS

Security tools for static analysis:

- Free / open source:

  Find security bugs, Phan, CAT.NET, Brakeman, Bandit, Flawfinder, QARK

- Commercial:

  HP Fortify, Checkmarx, Coverity, IBM AppScan Source, Klocwork, Veracode, Brakeman Pro

Security tools for vulnerable dependencies:

- Free / open source:

  OWASP Dependency Check, SafeNuGet, Retire.js

- Commercial:

  Sonatype, Black Duck, Palamida, Source Clear

SHIFTING SECURITY LEFT – CONTINUOUS DELIVERY

Automate various dynamic tests throughout the delivery pipeline:

- Functional security testing
  - Automate tests against authentication, authorization, password management using Selenium or similar tool
- Dynamic Application Security Testing (DAST)
  - Black box scanners looking for known classes of weakness
  - Library of past flaws to scan for

DYNAMIC ANALYSIS TOOLS

Security tools for dynamic analysis

- Free / open source:
  - ZAP, Arachni, w3af, Skipfish, Nikto
- Commercial:
  - Burp Suite, HP WebInspect, IMB AppScan, Nessus, Veracode, WhiteHat Sentinel
- CI Scanning frameworks:
  - Gauntlt, F-Secure, BDD-Security, Mozilla Minion, Yahoo Gryffin

SHIFTING SECURITY LEFT – CONTINUOUS MONITORING

Leverage monitoring tools and approaches for security monitoring:

- Look for attack signatures
  - Authentication failures, 4XX/5XX errors, database syntax errors, login failures, access control exceptions
- Correlate with traffic information (source, type)
- Feed trends and anomalies back to monitoring tools

Must watch: Christopher Rimondi "Using DevOps Monitoring Tools to Increase Security Visibility"

- https://www.youtube.com/watch?v=TNCVv9itQf4

CONTINUOUS MONITORING – DASHBOARD - Etsy

CONTINUOUS MONITORING - DASHBOARD

- Hygieia – Capitol One (https://github.com/capitalone/Hygieia)

Agenda

- Continuous Opportunity: DevOps & Security

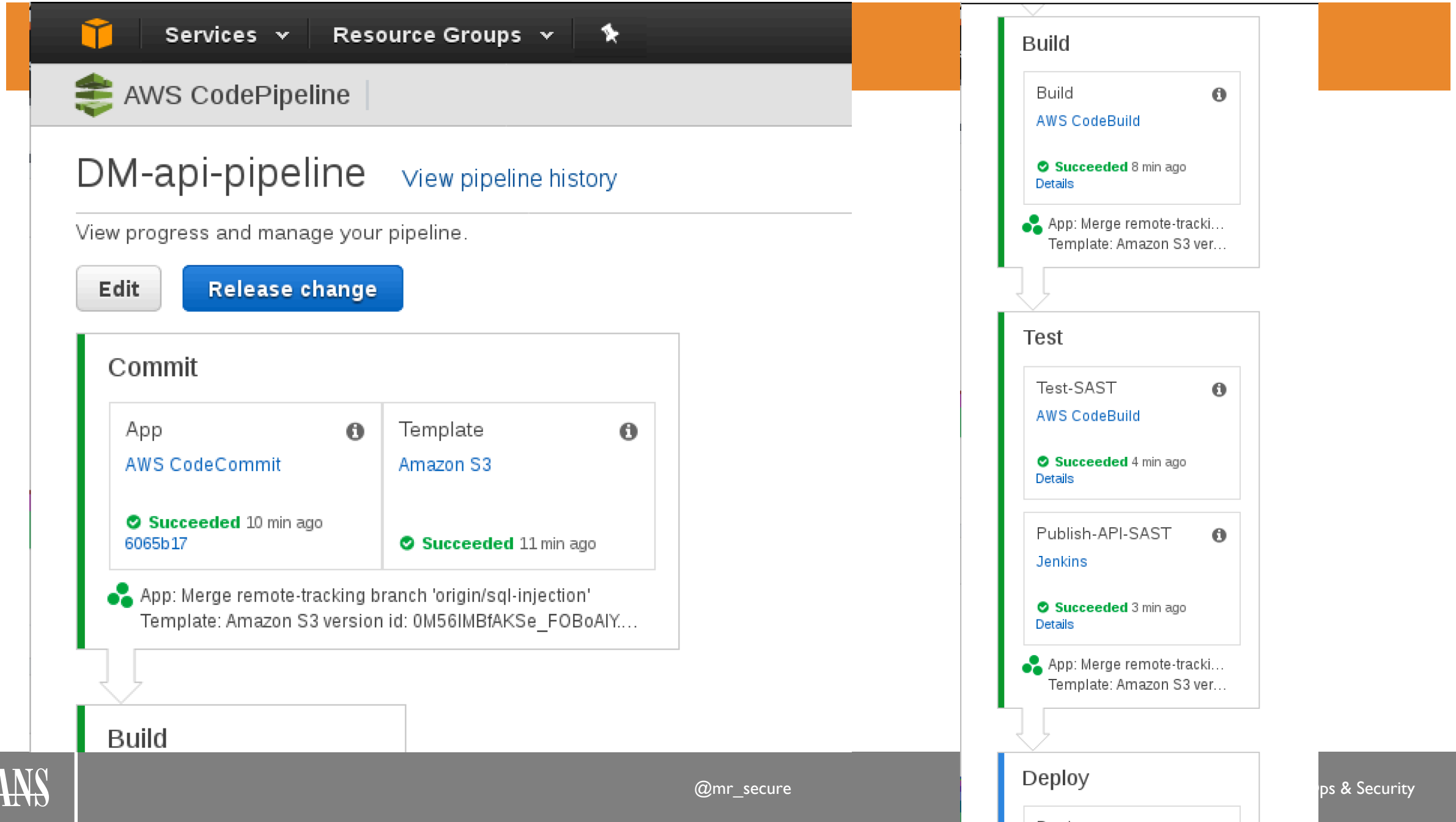
CONTINUOUS OPPORTUNITY

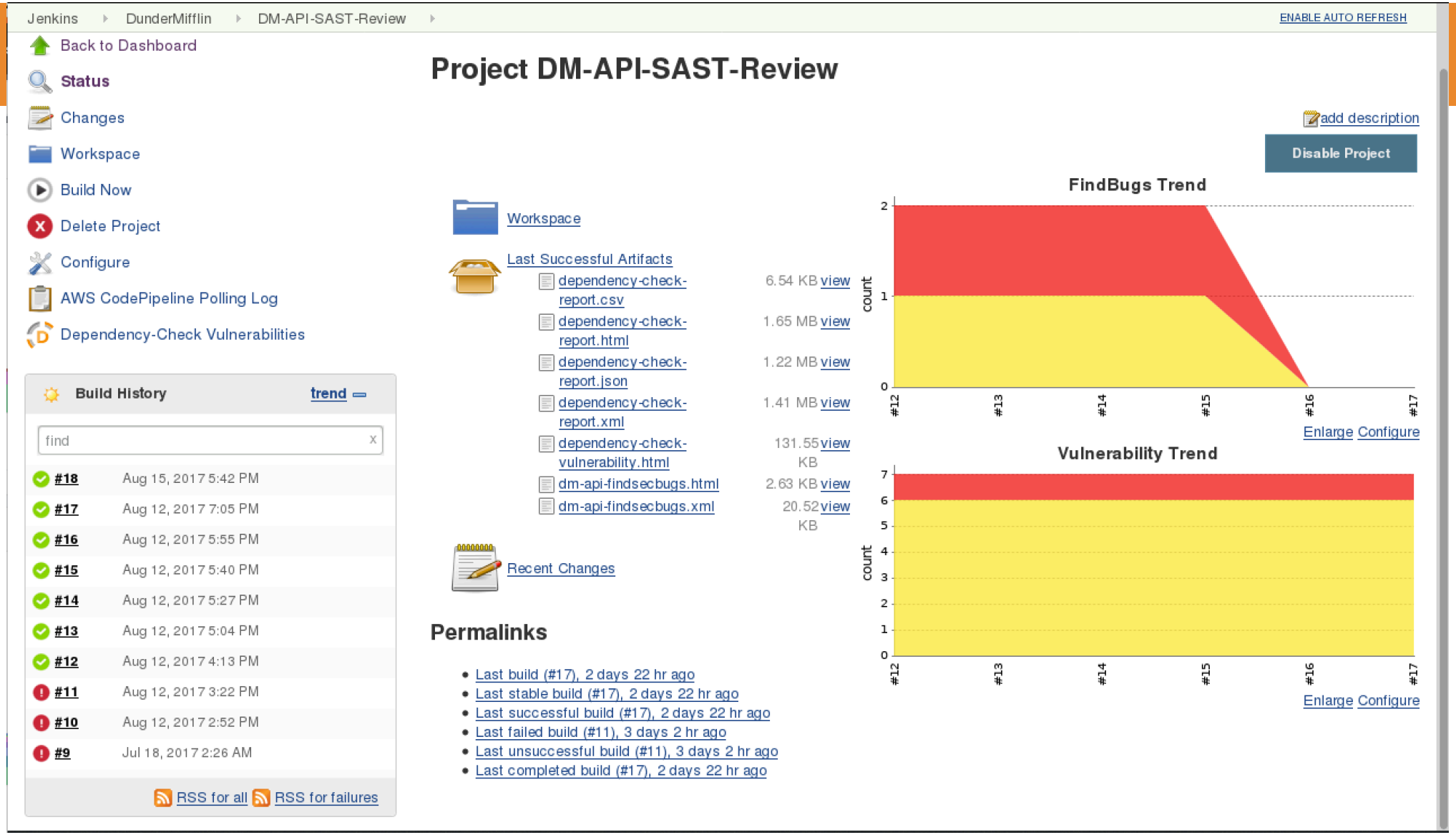
1. **The DevOps Movement**
2. **Shifting Security Left**
3. ***Examples***

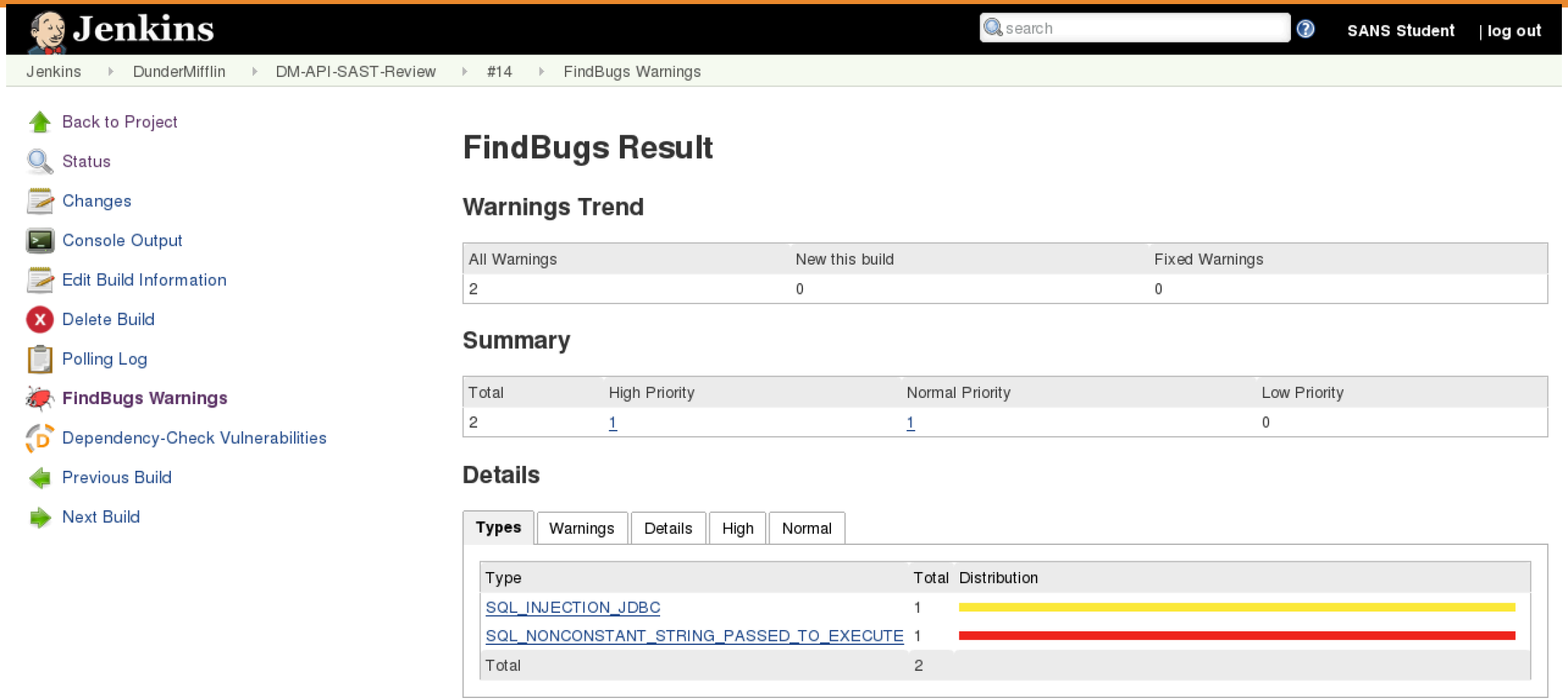
SHIFTING SECURITY LEFT

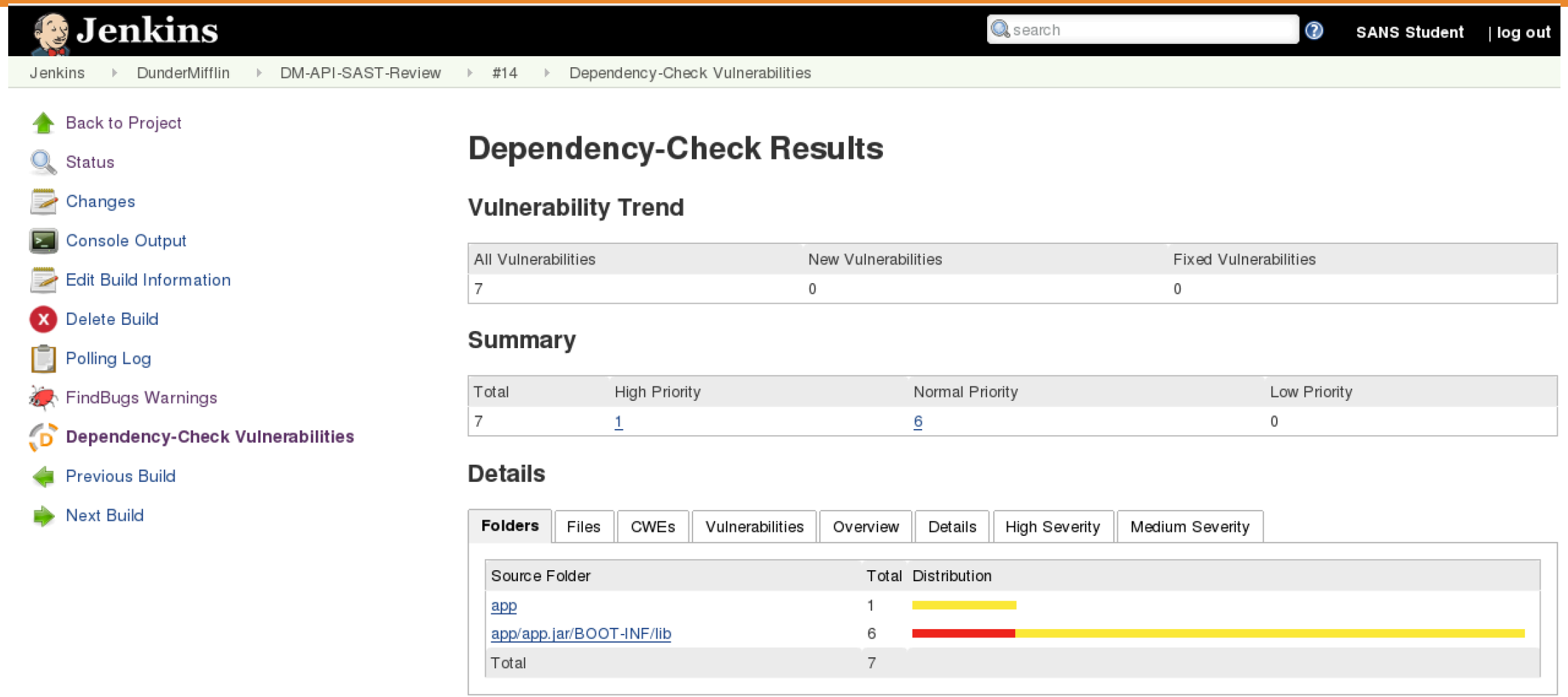
- AWS CodePipeline used to build Java App
- AWS CodeBuild ”Build” phase creates docker container
- AWS CodeBuild “Test” phase runs SAST, Dependency checks
- Data published into Jenkins

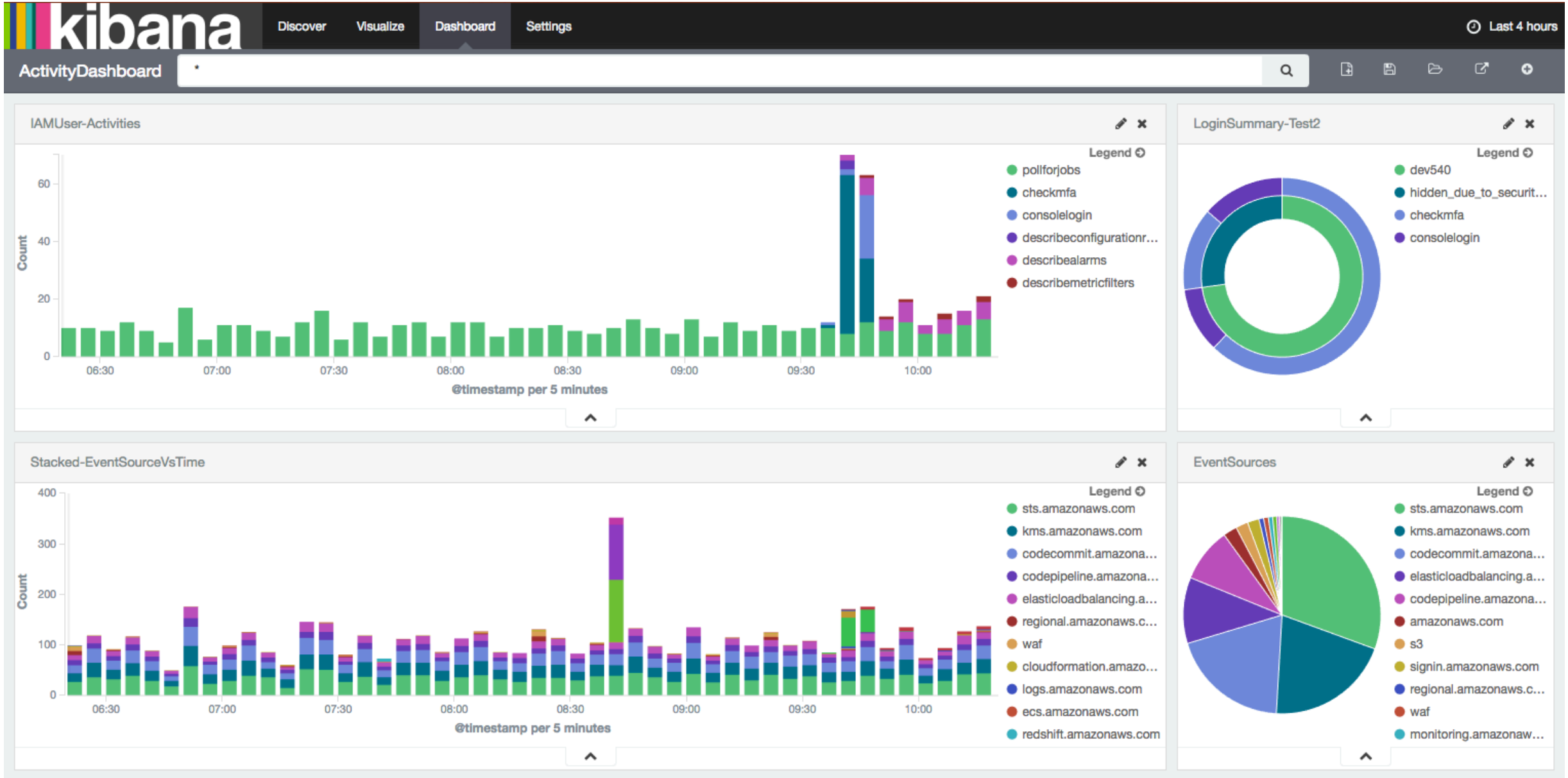
- Integrate security testing into the build process


Services
Resource Groups
AWS CodePipeline
DM-api-pipeline
View pipeline history
View progress and manage your pipeline.
Edit
Release change
Commit
App
AWS CodeCommit
Succeeded 10 min ago
6065b17
Template
Amazon S3
Succeeded 11 min ago
App: Merge remote-tracking branch 'origin/sql-injection'
Template: Amazon S3 version id: 0M56IMBfAKSe_FOBoAlY....
Build
Build
AWS CodeBuild
Succeeded 8 min ago
Details
App: Merge remote-tracki...
Template: Amazon S3 ver...
Test
Test-SAST
AWS CodeBuild
Succeeded 4 min ago
Details
Publish-API-SAST
Jenkins
Succeeded 3 min ago
Details
App: Merge remote-tracki...
Template: Amazon S3 ver...
Deploy


Jenkins
DunderMifflin
DM-API-SAST-Review
ENABLE AUTO REFRESH
Back to Dashboard
Status
Changes
Workspace
Build Now
Delete Project
Configure
AWS CodePipeline Polling Log
Dependency-Check Vulnerabilities
Build History
trend
find
#18 Aug 15, 2017 5:42 PM
#17 Aug 12, 2017 7:05 PM
#16 Aug 12, 2017 5:55 PM
#15 Aug 12, 2017 5:40 PM
#14 Aug 12, 2017 5:27 PM
#13 Aug 12, 2017 5:04 PM
#12 Aug 12, 2017 4:13 PM
#11 Aug 12, 2017 3:22 PM
#10 Aug 12, 2017 2:52 PM
#9 Jul 18, 2017 2:26 AM
RSS for all
RSS for failures
Project DM-API-SAST-Review
add description
Disable Project
Workspace
Last Successful Artifacts
dependency-check-report.csv 6.54 KB view
dependency-check-report.html 1.65 MB view
dependency-check-report.json 1.22 MB view
dependency-check-report.xml 1.41 MB view
dependency-check-vulnerability.html 131.55 KB view
dm-api-findsecbugs.html 2.63 KB view
dm-api-findsecbugs.xml 20.52 KB view
Recent Changes
Permalinks
Last build (#17), 2 days 22 hr ago
Last stable build (#17), 2 days 22 hr ago
Last successful build (#17), 2 days 22 hr ago
Last failed build (#11), 3 days 2 hr ago
Last unsuccessful build (#11), 3 days 2 hr ago
Last completed build (#17), 2 days 22 hr ago
FindBugs Trend
count
#12 #13 #14 #15 #16 #17
Enlarge Configure
Vulnerability Trend
count
#12 #13 #14 #15 #16 #17
Enlarge Configure


Jenkins
search
SANS Student
| log out
Jenkins
DunderMifflin
DM-API-SAST-Review
#14
FindBugs Warnings
Back to Project
Status
Changes
Console Output
Edit Build Information
Delete Build
Polling Log
FindBugs Warnings
Dependency-Check Vulnerabilities
Previous Build
Next Build
FindBugs Result
Warnings Trend
All Warnings
New this build
Fixed Warnings
2
0
0
Summary
Total
High Priority
Normal Priority
Low Priority
2
1
1
0
Details
Types
Warnings
Details
High
Normal
Type
Total
Distribution
SQL_INJECTION_JDBC
1
SQL_NONCONSTANT_STRING_PASSED_TO_EXECUTE
1
Total
2


Jenkins
search
SANS Student
| log out
Jenkins ▸ DunderMifflin ▸ DM-API-SAST-Review ▸ #14 ▸ Dependency-Check Vulnerabilities
Back to Project
Status
Changes
Console Output
Edit Build Information
Delete Build
Polling Log
FindBugs Warnings
Dependency-Check Vulnerabilities
Previous Build
Next Build
Dependency-Check Results
Vulnerability Trend
All Vulnerabilities
New Vulnerabilities
Fixed Vulnerabilities
7
0
0
Summary
Total
High Priority
Normal Priority
Low Priority
7
1
6
0
Details
Folders
Files
CWEs
Vulnerabilities
Overview
Details
High Severity
Medium Severity
Source Folder
Total
Distribution
app
1
app/app.jar/BOOT-INF/lib
6
Total
7

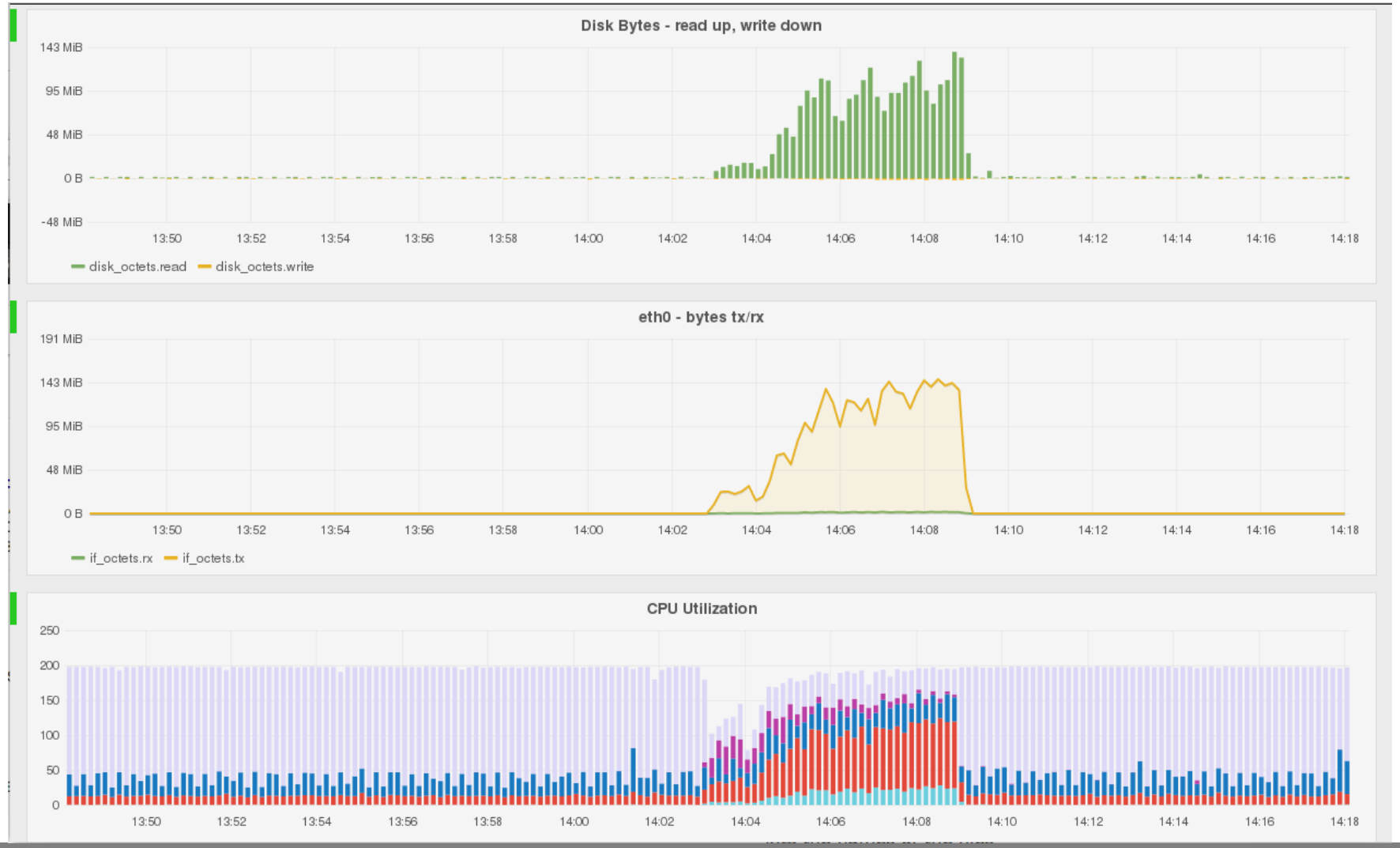

kibana
Discover
Visualize
Dashboard
Settings
Last 4 hours
ActivityDashboard
*
IAMUser-Activities
Legend
pollforjobs
checkmfa
consolelogin
describeconfigurationr...
describealarms
describemetricfilters
Count
0
20
40
60
06:30
07:00
07:30
08:00
08:30
09:00
09:30
10:00
@timestamp per 5 minutes
LoginSummary-Test2
Legend
dev540
hidden_due_to_securit...
checkmfa
consolelogin
Stacked-EventSourceVsTime
Legend
sts.amazonaws.com
kms.amazonaws.com
codecommit.amazona...
codepipeline.amazona...
elasticloadbalancing.a...
regional.amazonaws.c...
waf
cloudformation.amazo...
logs.amazonaws.com
ecs.amazonaws.com
redshift.amazonaws.com
Count
0
100
200
300
400
06:30
07:00
07:30
08:00
08:30
09:00
09:30
10:00
@timestamp per 5 minutes
EventSources
Legend
sts.amazonaws.com
kms.amazonaws.com
codecommit.amazona...
elasticloadbalancing.a...
codepipeline.amazona...
amazonaws.com
s3
signin.amazonaws.com
regional.amazonaws.c...
waf
monitoring.amazonaw...

MONITORING FOR SECURITY

- Backstory:
  - Basic OS-level monitoring on hosts
  - Using collectd to gather disk/cpu/network stats & ship to graphite
- What can we identify?

- Note: These data sets are based on simulations, not actual incidents

Data Exfiltration?



Ransomware?


Disk Bytes - read up, write down
48 MiB
0 B
-48 MiB
-95 MiB
-143 MiB
12:32
12:34
12:36
12:38
12:40
12:42
12:44
12:46
12:48
12:50
12:52
12:54
12:56
12:58
disk_octets.read
disk_octets.write
eth0 - bytes tx/rx
2.0 KiB
1.5 KiB
1000 B
500 B
0 B
if_octets.rx
if_octets.tx
CPU Utilization
250
200
150
100
50
0

PARTING THOUGHTS

Opportunities that SecDevOps presents:

- Trade inefficient, ineffective point-in-time compliance snapshots for continuous, real-time verification
- Build security testing, scanning, and reviews into the pipeline to find low hanging fruit & prevent regressions
- Reduce time spent on security remediation
- Ensure the entire project team understands the hostile environment their applications face via continuous feedback from production

Questions ?

SANS AppSec
APPLICATION & SOFTWARE SECURITY

C U R R I C U L U M

Get the right training to build secure applications.

PLATFORM SECURITY

DEV531
Defending Mobile Applications Security Essentials

DEV541
Secure Coding in Java/JEE
GSSP-JAVA

DEV544
Secure Coding in .NET
GSSP-NET

CORE

STH.DEVELOPER
Application Security Awareness Modules

DEV522
Defending Web Applications Security Essentials
GWEB

DEV534
Secure DevOps: A Practical Introduction

SEC540
Secure DevOps and Cloud Application Security

SPECIALIZATION

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing and Ethical Hacking

ASSESSMENT

AppSec CyberTalent Assessment
sans.org/appsec-assessment

@sansappsec

software-security.sans.org

CREDITS

SPEAKER
Ben Allen
ben.allen@mrsecure.org
@mr_secure

AUTHORS
Jim Bird
@jimrbird

Ben Allen
@mr_secure

DEVELOPER RESOURCES
software-security.sans.org
Twitter: @sansappsec

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org