Dev-First Security

Guy Podjarny

Co-Founder & President

Snyk

About Me

- Guy Podjarny, *@guypod*
- Co-Founder & President at *Snyk*
- CTO at *Akamai*
  - Focusing on Web Performance & Scale
- Co-founder & CTO at *Blaze.io*
  - Make websites faster!
- Built early App Sec products
  - AppShield (first WAF), AppScan (first DAST, SAST)
  - Sanctum, acq by Watchfire, acq by IBM

- Host *The Secure Developer* Podcast
- O'Reilly Author
  - Securing Open Source Libraries
  - Serverless Security
  - High Performance Images
  - Responsive & Fast

Free Copy:
https://info.snyk.io/oreilly-lp

Free Copy:
https://info.snyk.io/oreilly-serverless-security

Digital Transformation

What is digital transformation?

More Software

Cloud technologies

DevOps methodologies

More Software = More Software Risk

> “For many companies cybersecurity is increasingly a critical business issue, not only or even primarily a technology issue…
> Hedge-funds… didn’t use to care about cybersecurity.
> Now they’re obsessed with it.”

James Kaplan

McKinsey, Cybersecurity Leader

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Cloud reshapes applications

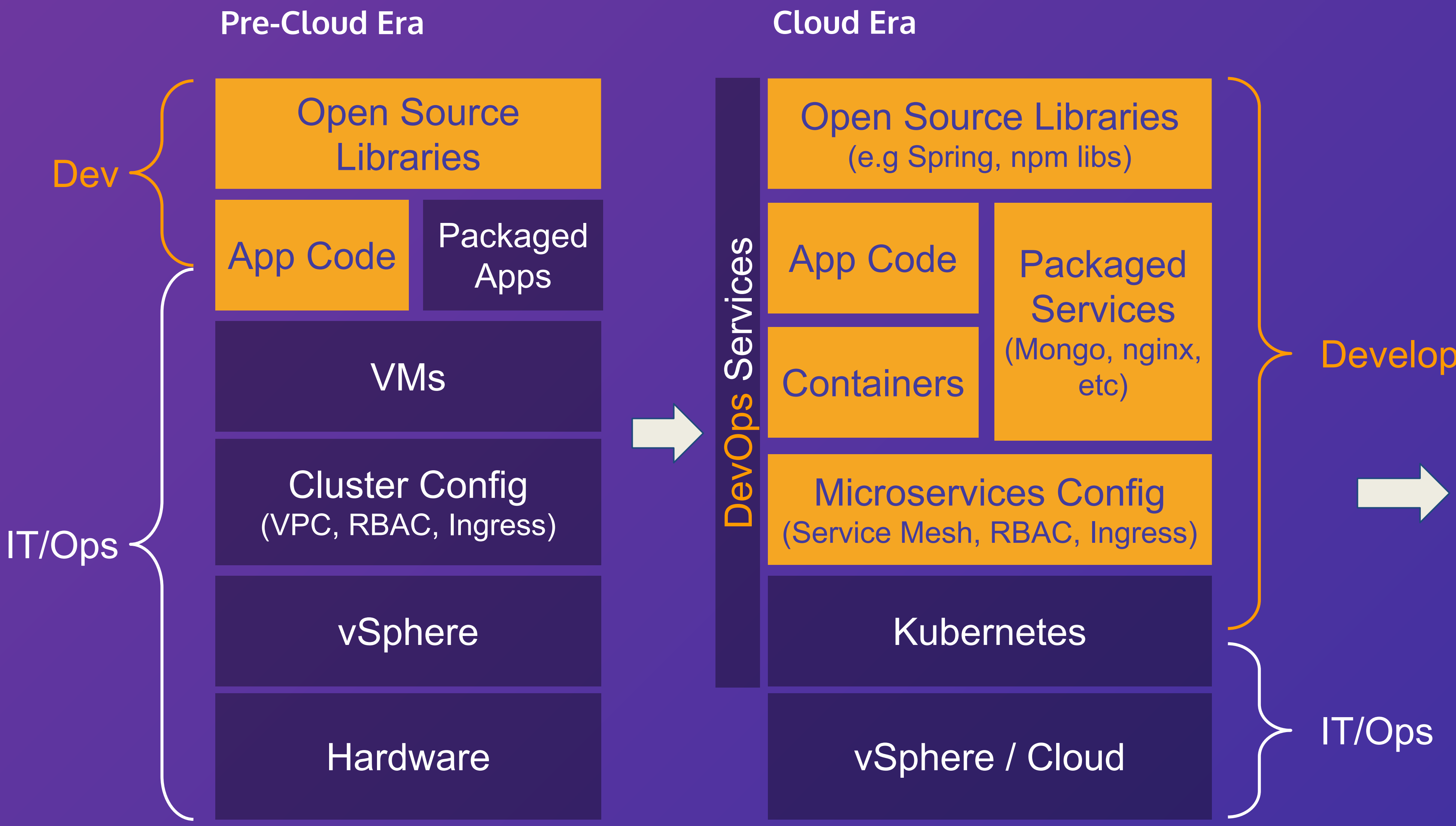
New tech:
Containers, Serverless,
Open Source…

Less mature tech,
changing rapidly

Data center security
Replaced with config

Cloud changes the
scope of the application

Cloud transforms *IT* into *App*



Pre-Cloud Era

Dev

Open Source Libraries

App Code

Packaged Apps

IT/Ops

VMs

Cluster Config
(VPC, RBAC, Ingress)

vSphere

Hardware

Cloud Era

DevOps Services

Open Source Libraries
(e.g Spring, npm libs)

App Code

Containers

Packaged Services
(Mongo, nginx, etc)

Microservices Config
(Service Mesh, RBAC, Ingress)

Kubernetes

vSphere / Cloud

Developer

IT/Ops

- Data
- Delivery (CDN)
- API Gateway
- 3rd Party Services
- ...

Moving into the app!

IT/Infra

App/Developer

DevOps changes process & ownership

1

Continuous Integration & Delivery

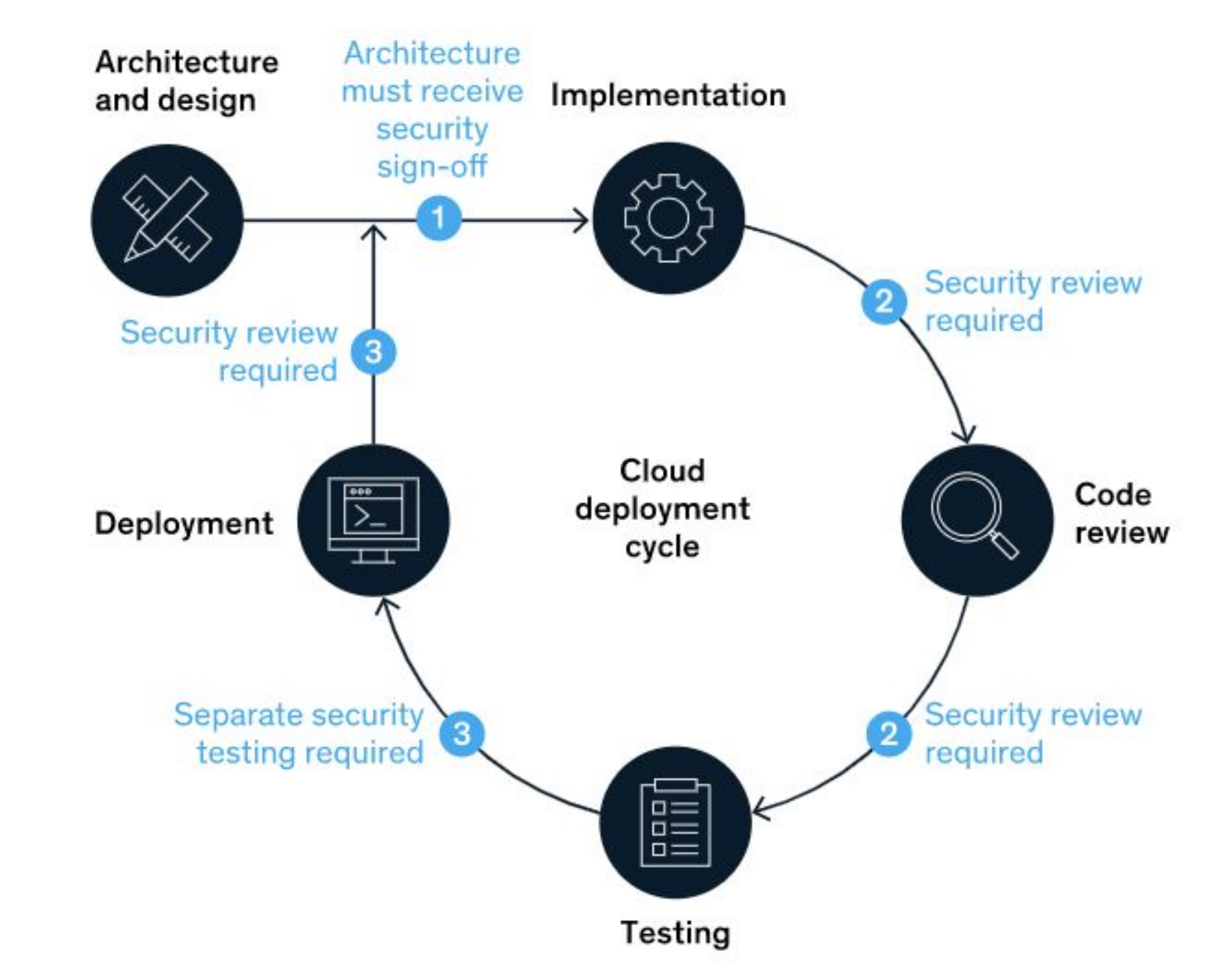
No manual gates/delay

2

Empowered, self-sufficient Dev teams

own journey end to end

Security is left behind

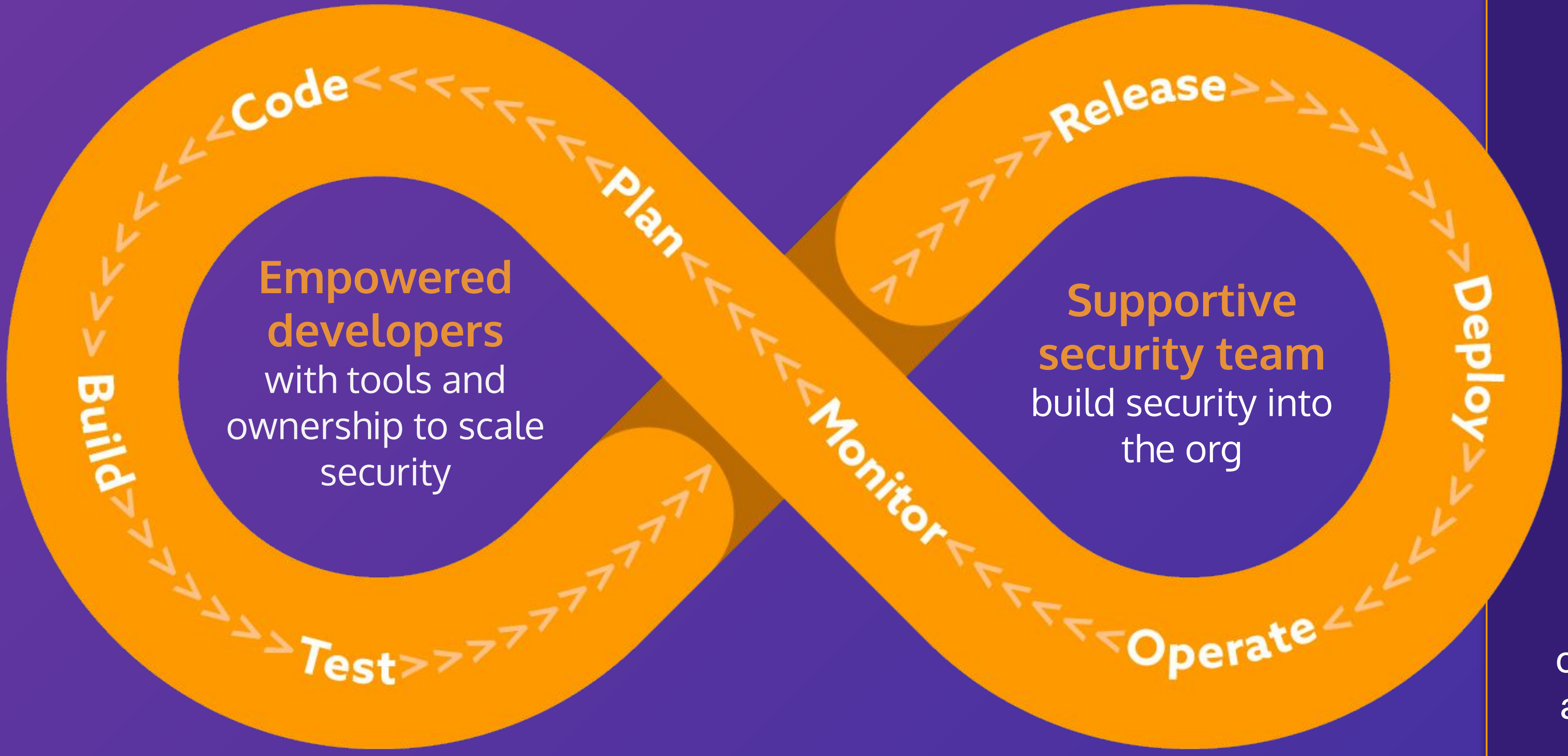


- **Security teams in** **critical delivery path,** slowing the business down
- Security teams siloed & **out of the loop,** resulting in insecure apps
- Talent shortage **perpetuates state** of understaffed Security teams

Solution:
Dev-First Security

“Shift left” is not enough

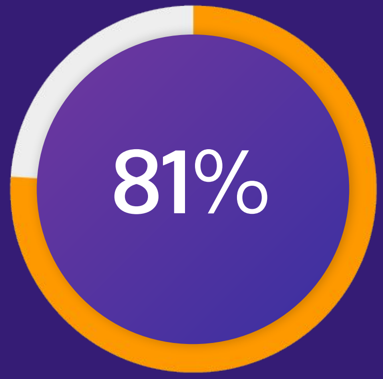
Real change is “top to bottom”: Shift ownership to empowered teams



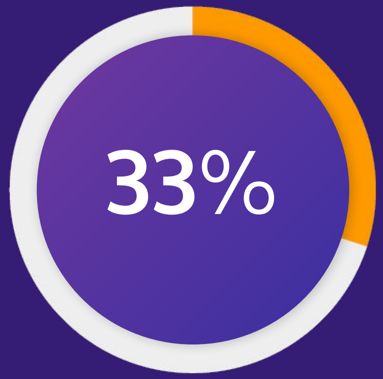
Empowered developers with tools and ownership to scale security

Supportive security team build security into the org

Snyk DevSecOps Insights 2020



of respondents believe developers should actually own security, but they aren't well-equipped to do so.

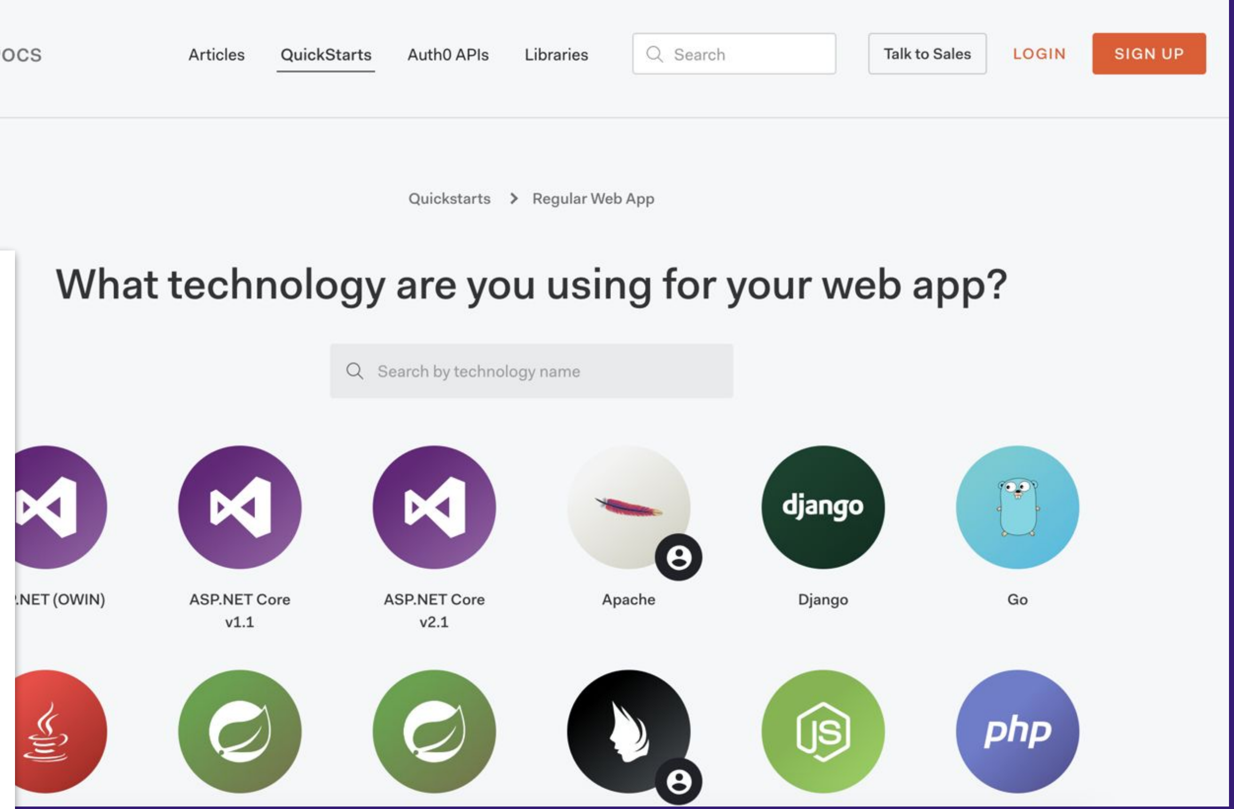


of respondents feel that security is a major constraint on the ability to deliver software quickly.

snyk

Empowered Developers

Enable successful self-serve usage



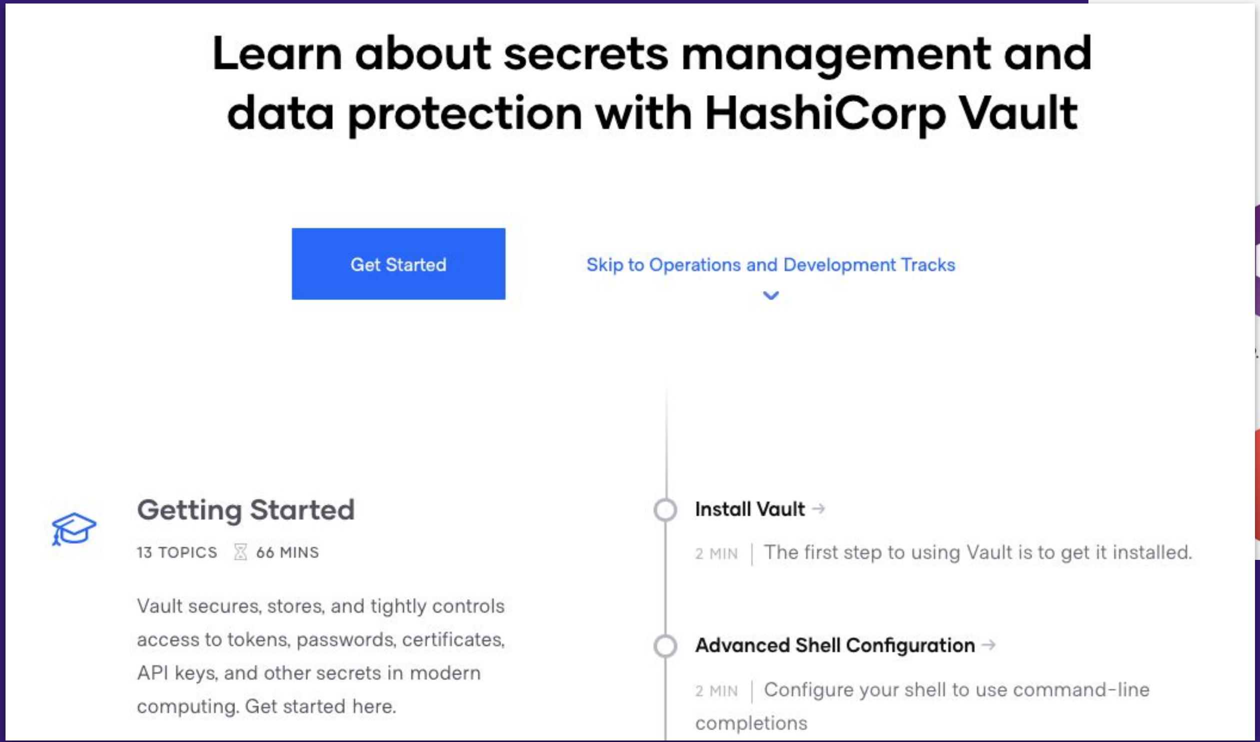
Auth0 Docs

Articles QuickStarts Auth0 APIs Libraries Search Talk to Sales LOGIN SIGN UP

Quickstarts > Regular Web App

What technology are you using for your web app?

Search by technology name



Learn about secrets management and data protection with HashiCorp Vault

Get Started

Skip to Operations and Development Tracks

Getting Started

13 TOPICS 66 MINS

Vault secures, stores, and tightly controls access to tokens, passwords, certificates, API keys, and other secrets in modern computing. Get started here.

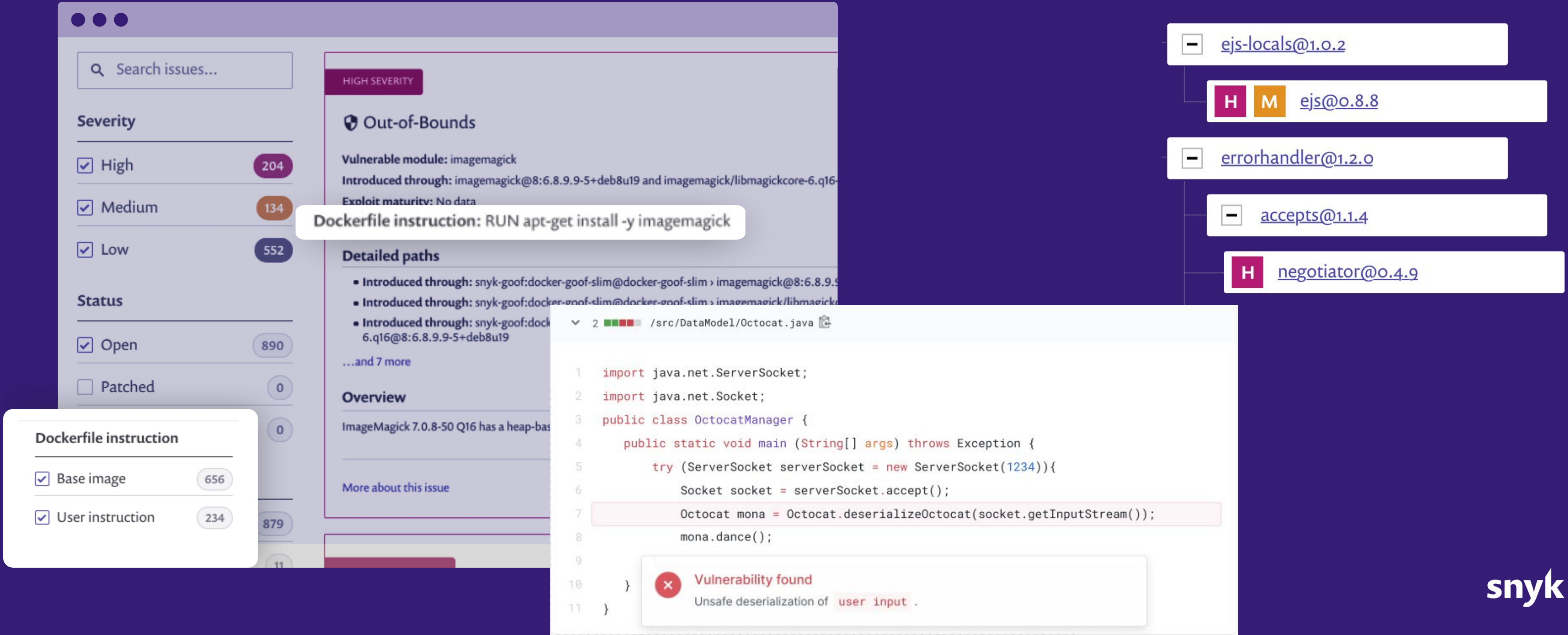
Install Vault →

2 MIN | The first step to using Vault is to get it installed.

Advanced Shell Configuration →

2 MIN | Configure your shell to use command-line completions

Explain how a vulnerability made it in



Search issues...

Severity

- ☑ High 204
- ☑ Medium 134
- ☑ Low 552

Status

- ☑ Open 890
- □ Patched 0
- 0

879

Dockerfile instruction

- ☑ Base image 656
- ☑ User instruction 234

HIGH SEVERITY

Out-of-Bounds

Vulnerable module: imagemagick
Introduced through: imagemagick@8:6.8.9.9-5+deb8u19 and imagemagick/libmagickcore-6.q16-
Exploit maturity: No data

Dockerfile instruction: RUN apt-get install -y imagemagick

Detailed paths

- **Introduced through:** snyk-goof:docker-goof-slim@docker-goof-slim › imagemagick@8:6.8.9.9
- **Introduced through:** snyk-goof:docker-goof-slim@docker-goof-slim › imagemagick/libmagickc
- **Introduced through:** snyk-goof:dock 6.q16@8:6.8.9.9-5+deb8u19

…and 7 more

Overview

ImageMagick 7.0.8-50 Q16 has a heap-bas

More about this issue

2 /src/DataModel/Octocat.java

```
import java.net.ServerSocket;
import java.net.Socket;
public class OctocatManager {
  public static void main (String[] args) throws Exception {
      try (ServerSocket serverSocket = new ServerSocket(1234)){
          Socket socket = serverSocket.accept();
          Octocat mona = Octocat.deserializeOctocat(socket.getInputStream());
          mona.dance();

      }
}
```

Vulnerability found
Unsafe deserialization of `user input`.

- ejs-locals@1.0.2
  - H M ejs@0.8.8
- errorhandler@1.2.0
  - accepts@1.1.4
    - H negotiator@0.4.9

snyk

Train dev with your own vulns

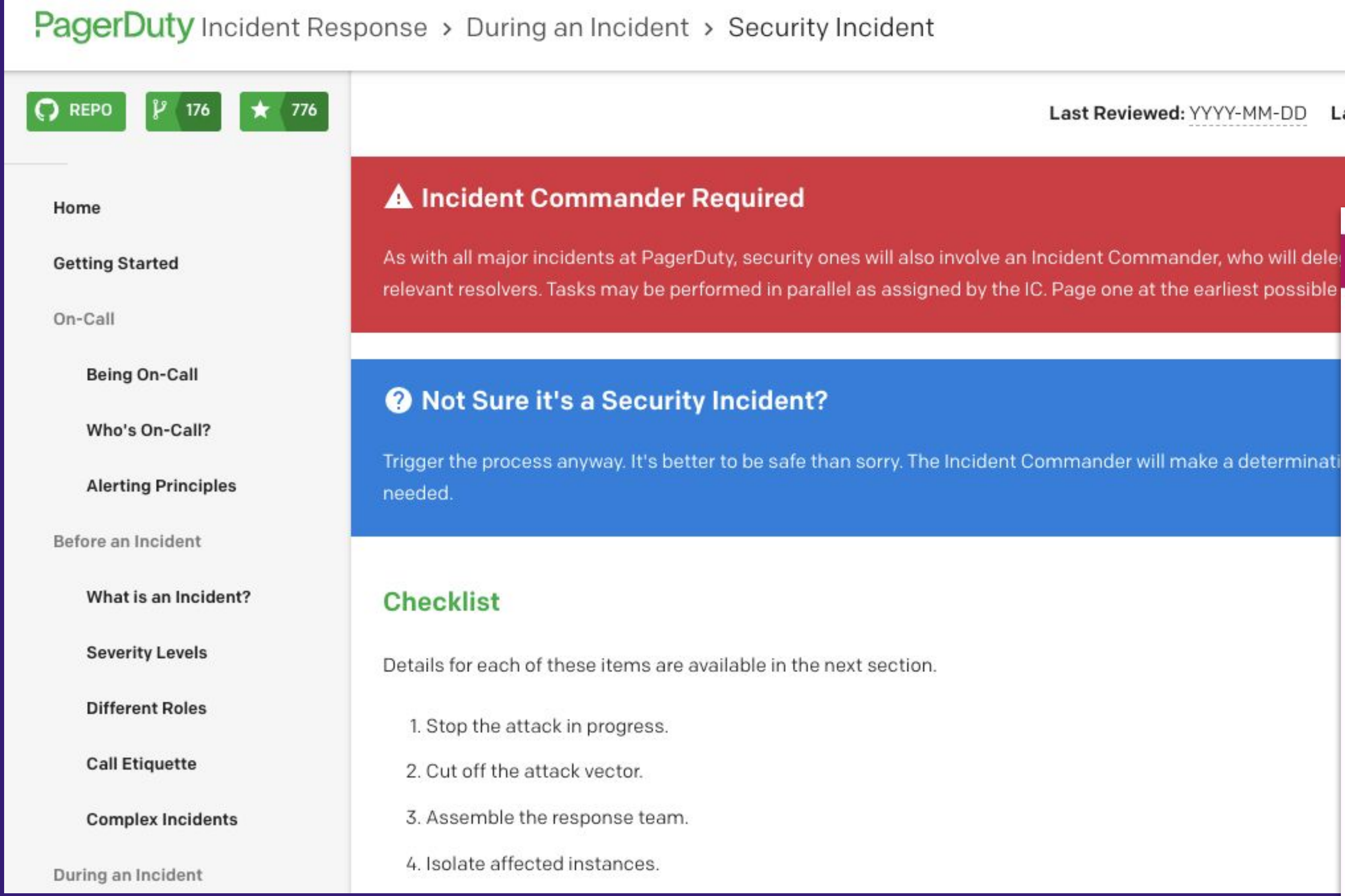
> When developers start at Segment they go through a two part training. The first part is thinking like an attacker... Every single example that we show them is something that was ***a vulnerability that was previously in Segment***....
>
> ... it's ***a lot easier to get a developer to care*** about a vulnerability when you can say, "This feature that you're probably familiar with, this was a previous vulnerability. This was the impact. This is what the fix looked like."

Eric Ellett, Leif Dreizler

Segment, Security Engineering

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Provide security questions, and answers



Last Reviewed: YYYY-MM-DD **Last Tested:** YYYY-MM-DD

Incident Commander Required

As with all major incidents at PagerDuty, security ones will also involve an Incident Commander, who will dele relevant resolvers. Tasks may be performed in parallel as assigned by the IC. Page one at the earliest possible

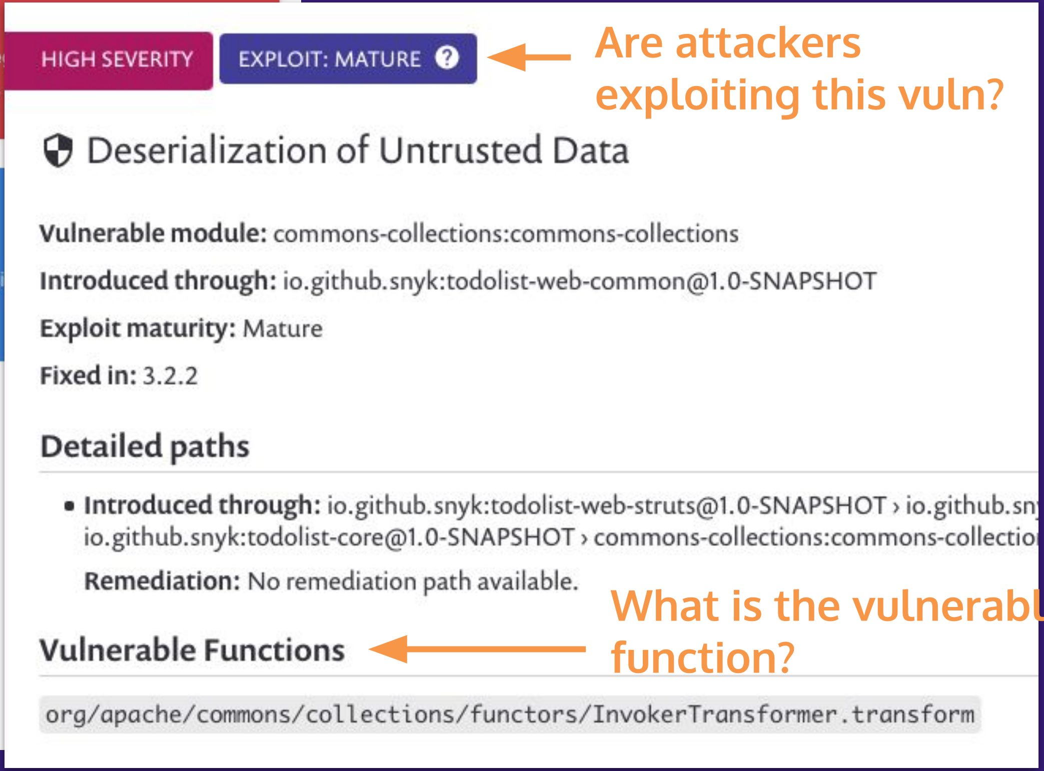
Not Sure it's a Security Incident?

Trigger the process anyway. It's better to be safe than sorry. The Incident Commander will make a determinati needed.

Checklist

Details for each of these items are available in the next section.

1. Stop the attack in progress.
2. Cut off the attack vector.
3. Assemble the response team.
4. Isolate affected instances.



Are attackers exploiting this vuln?

Deserialization of Untrusted Data

Vulnerable module: commons-collections:commons-collections

Introduced through: io.github.snyk:todolist-web-common@1.0-SNAPSHOT

Exploit maturity: Mature

Fixed in: 3.2.2

Detailed paths

- **Introduced through:** io.github.snyk:todolist-web-struts@1.0-SNAPSHOT › io.github.sn io.github.snyk:todolist-core@1.0-SNAPSHOT › commons-collections:commons-collectio

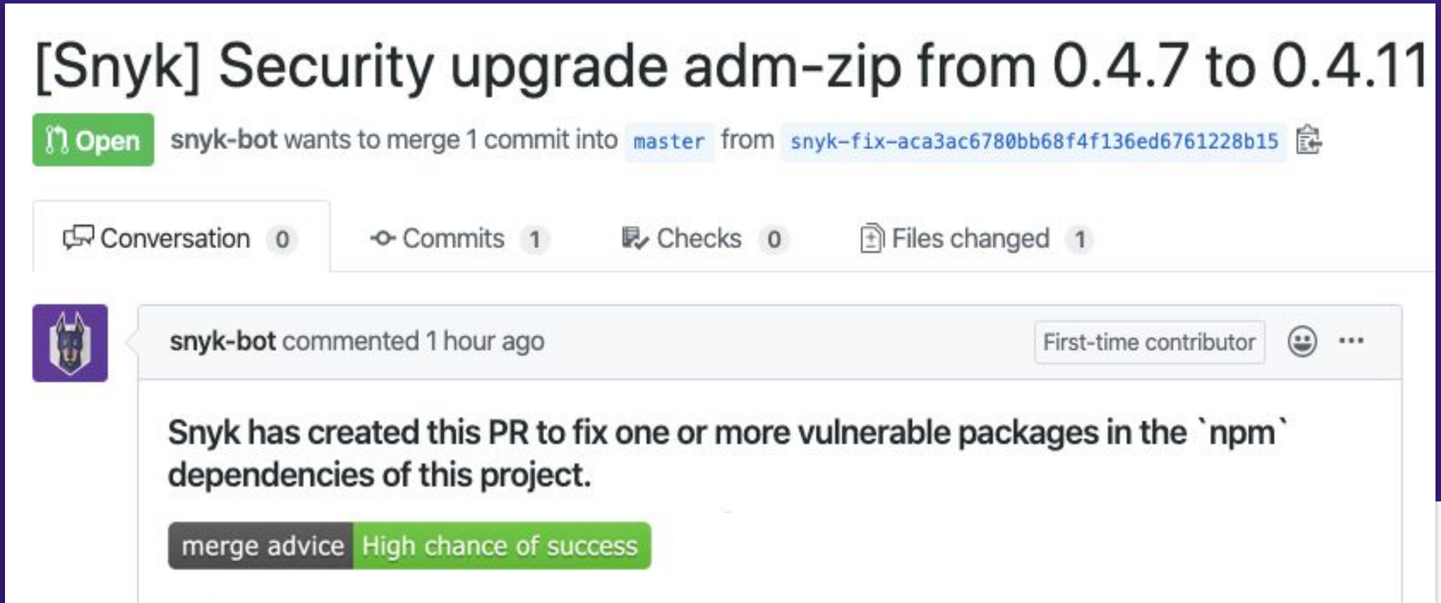
  Remediation: No remediation path available.

Vulnerable Functions

What is the vulnerable function?

```
org/apache/commons/collections/functors/InvokerTransformer.transform
```

Don’t just find issues, fix them!



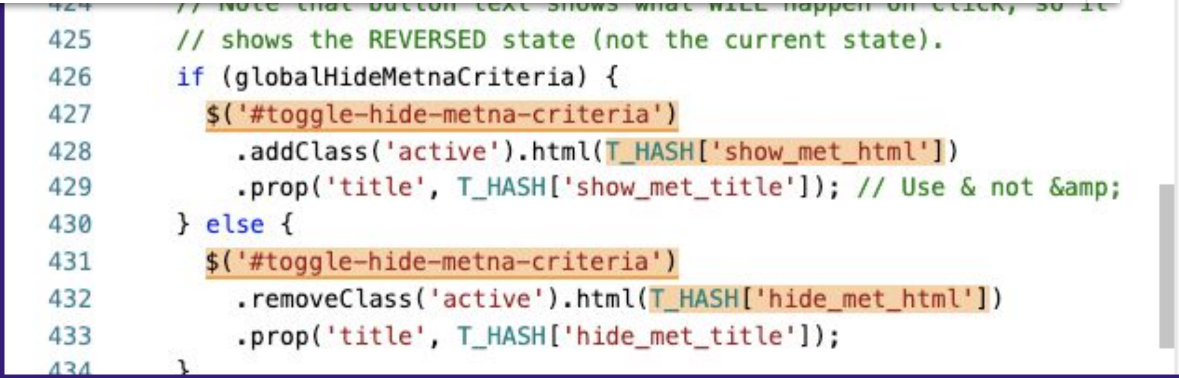
[Snyk] Security upgrade adm-zip from 0.4.7 to 0.4.11

snyk-bot wants to merge 1 commit into `master` from `snyk-fix-aca3ac6780bb68f4f136ed6761228b15`

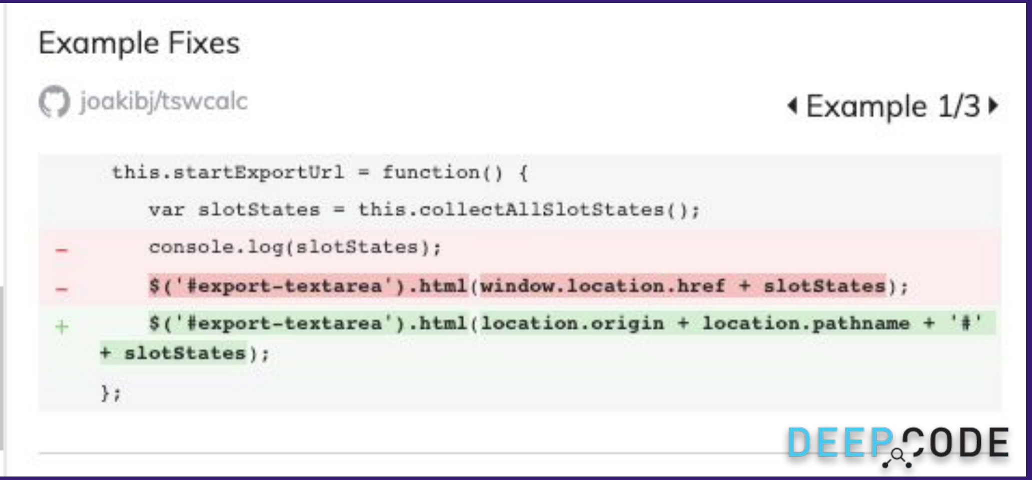
snyk-bot commented 1 hour ago

Snyk has created this PR to fix one or more vulnerable packages in the `npm` dependencies of this project.

merge advice | High chance of success



```
// Note that button text shows what WILL happen on click, so it
// shows the REVERSED state (not the current state).
if (globalHideMetnaCriteria) {
  $('#toggle-hide-metna-criteria')
    .addClass('active').html(T_HASH['show_met_html'])
    .prop('title', T_HASH['show_met_title']); // Use & not &amp;
} else {
  $('#toggle-hide-metna-criteria')
    .removeClass('active').html(T_HASH['hide_met_html'])
    .prop('title', T_HASH['hide_met_title']);
}
```



Example Fixes

joakibj/tswcalc

```
 this.startExportUrl = function() {
     var slotStates = this.collectAllSlotStates();
-    console.log(slotStates);
-    $('#export-textarea').html(window.location.href + slotStates);
+    $('#export-textarea').html(location.origin + location.pathname + '#'
 + slotStates);
 };
```

Automate your remediation flow

> “Deployed an internal tool that looks at the latest version of the [internal golden] base image… and ***creates PRs to update*** the FROM statement in the Dockerfile…
> around 65% of the PRs we created so far were merged or closed…
> When you ***make the task as simple as possible, they do the right thing***”

Yashivier Kosaraju

Twilio, Head of Product Security

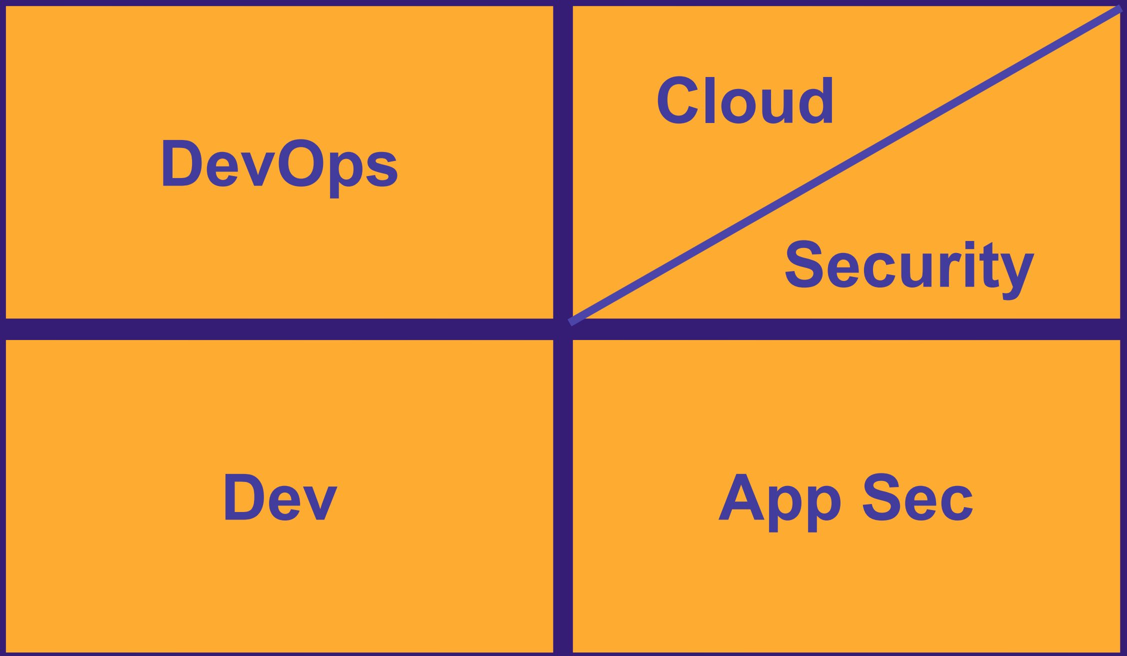
Snyk.io

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

snyk

Supportive Security

Align security org to Dev & Ops orgs



DevOps

Cloud

Security

Dev

App Sec

- Organizational change
- Skillset change
- Mindset change

Organizational change

> “We have an AppSec person aligned with all of our engineering teams, especially the ones that do development…
> I attend stand ups for the team, so I know what's going on and I actually participate in the stand up with them.”

Sara Dunnack

Invision Application Security

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Skillset change

> “I would say a security team's staff will rotate about a third, maybe half, from process management that we do today generally into developers. But, what does that do to the security workforce?
> I think that's a big impact that will be going on for 10-15 years.”

Justin Somaini

CISO Yahoo!, Symantec, Box, SAP

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Mindset change

> “The way I like to characterize [the relationship between DevOps & Security] today is they’re frenemies…
>
> I think it’s inevitable that they’re going to have to partner more and ideally it would not be an antagonistic relationship”

Kelly Shortridge

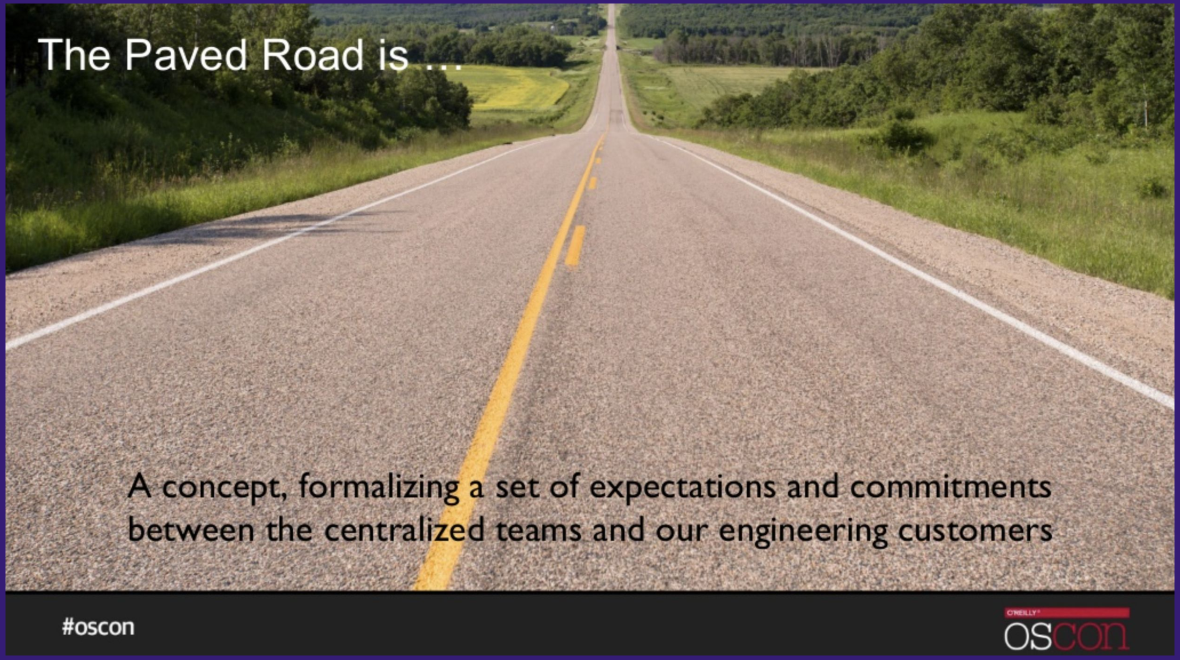
Capsule8 VP Product Strategy

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Make Security Easy on the Paved Road

"A concept, formalizing a set of expectations and commitments between the centralized teams and our engineering customers"

"Well-integrated, supported machinery to enable engineers to focus on delivering their core business value and to socialize the centralized team's support"



The Paved Road is …

A concept, formalizing a set of expectations and commitments between the centralized teams and our engineering customers

#oscon

The Paved Road provides …

Well-integrated, supported machinery to enable engineers to focus on delivering their core business value and to socialize the centralized team's support

#oscon

Source: https://www.slideshare.net/diannemarsh/the-paved-road-at-netflix

> “We call that concept "A paved road." You could certainly bushwhack and make your way through the woods. But if you have this nice smooth paved road that gets you to your destination, you're likely to opt in there.
> Now with freedom of responsibility we do preserve the individual decision making to go off that, but then they become responsible for that ”

Jason Chan

Netflix, VP Information Security

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Celebrate Security Success

> “At Salesforce we definitely tried a range of positive incentives, and I've carried that on to One Medical. Part of it is simply high-fiving somebody for doing the right thing. Part of it might be, everybody loves swag...
> Empowering software engineers and letting them make decisions, but also recognizing them for their good decisions and good work produces way better security than not.”

Zach Powers

One Medical, CISO

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Invest in Security Recognition

> “We have a *friendly neighborhood security bot* that reaches out to people on chat and says everything from, “Thanks for updating your phone to the latest release. You are one of the first few people to do that. You’re doing your part to keep us secure,” to *providing, in some cases, spot bonuses* to people who raise their hand and say, “Hey, there’s a problem over here and I want to be in front of it from a security standpoint.””

Mike Hanley

Duo (Cisco), Head of Security

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

“*Mike*: even little things like the first folks to report a phishing email that come in to the security team will sometimes give them a special kind of edition sticker that says they were the first to report a phishing or attack campaign on the organization

Me: That’s awesome. I think any good rewarding system should definitely involve stickers”

Mike Hanley

Duo (Cisco), Head of Security

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

Digital Transformation is happening
And Security is left behind

Transform Security into Dev-First Security

Cloud lets us reimagine security

> “I got a call from Google at the time… and he said “You know, Android is coming up strong and we need to figure out security and make sure that we do it right.” That for me was really a seminal moment because for me, it was clear that mobile was an opportunity to completely reset how we thought about security…
> I think the shift to cloud is a similar fundamental shift for companies… a There’s a shift in what we think is possible”

Adrian Ludwig

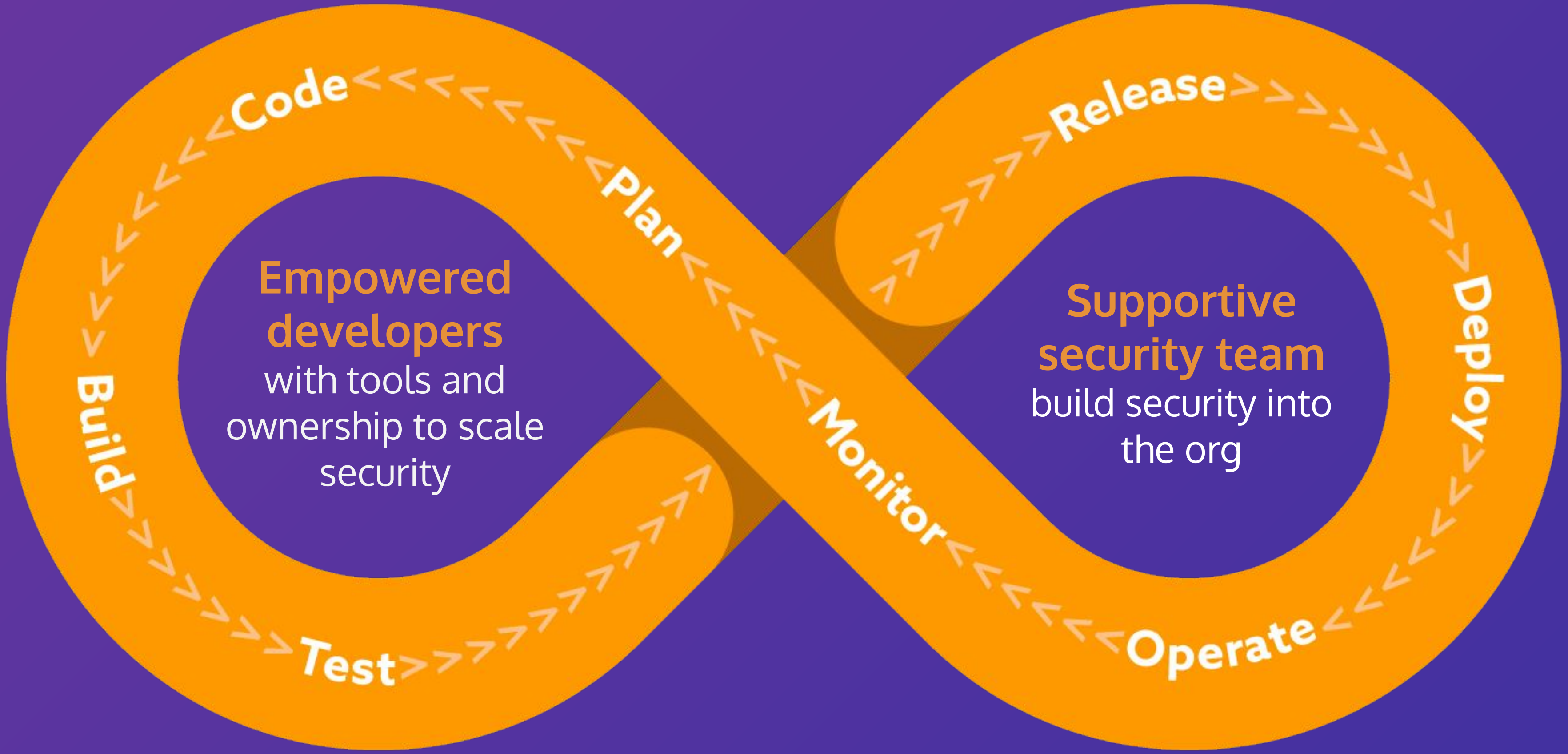
Atlassian, CISO

Snyk.io

Source: The Secure Developer Podcast (https://www.mydevsecops.io/the-secure-developer-podcast)

snyk

Dev-first security



Empowered developers with tools and ownership to scale security

Supportive security team build security into the org

Dev-First Security

Guy Podjarny

Co-Founder & President

Snyk