SYNOPSYS®

Welcome to the CISO UNIVERSE

Issue No. 1

THE CISO'S TERRIBLE, HORRIBLE, NO GOOD, VERY BAD DAY

*It's only **6:40 a.m.** and already, Alex, CISO of FilmFestFun, is having a bad day.*

"Attention passengers: All trains are delayed 45 minutes due to track issues. Thank you for your patience."

Oh no! I can't be late, not today!

Why haven't I gotten a Slack message about a successful build?

Forget the train, I'll take an Uber.

#!!@!

SURGE PRICING

Demand is off the charts! Rates have increased to get more Ubers on the road.

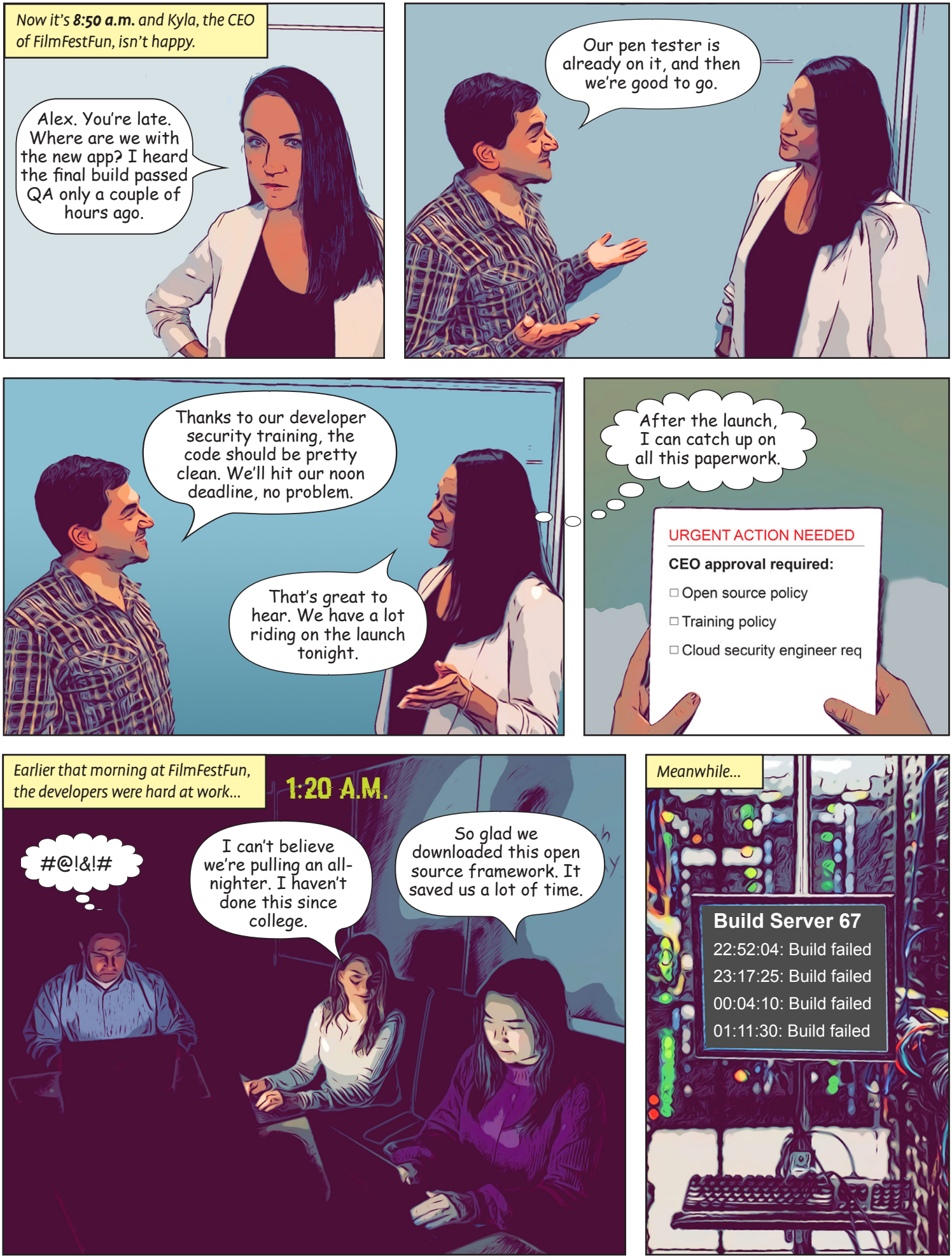
7.75X

THE NORMAL RATE

$93 MINIMUM FARE + $23.25 / MILE

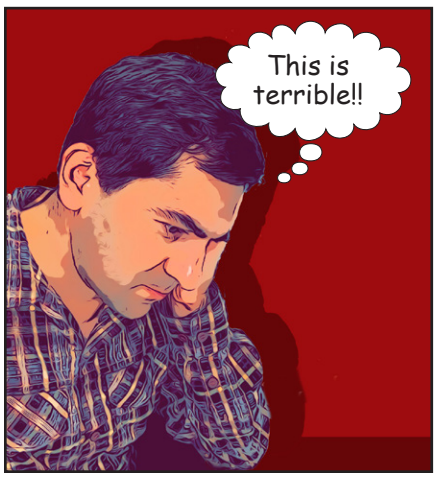
$5.81 / MIN

CONFIRM UBERX


Now it's 8:50 a.m. and Kyla, the CEO of FilmFestFun, isn't happy.
Alex. You're late. Where are we with the new app? I heard the final build passed QA only a couple of hours ago.
Our pen tester is already on it, and then we're good to go.
Thanks to our developer security training, the code should be pretty clean. We'll hit our noon deadline, no problem.
That's great to hear. We have a lot riding on the launch tonight.
After the launch, I can catch up on all this paperwork.
URGENT ACTION NEEDED
CEO approval required:
☐ Open source policy
☐ Training policy
☐ Cloud security engineer req
Earlier that morning at FilmFestFun, the developers were hard at work...
1:20 A.M.
#@!&!#
I can't believe we're pulling an all-nighter. I haven't done this since college.
So glad we downloaded this open source framework. It saved us a lot of time.
Meanwhile...
Build Server 67
22:52:04: Build failed
23:17:25: Build failed
00:04:10: Build failed
01:11:30: Build failed

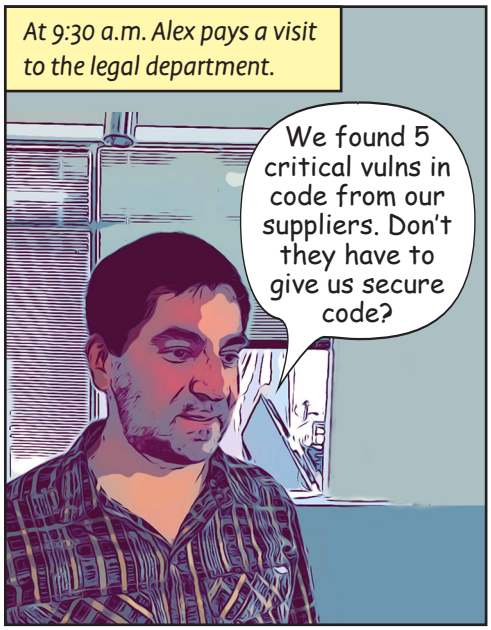
239 vulnerabilities found
22 critical
- 4 local code
- 5 contractor code
- 6 open source code
- 3 design
- 4 cloud configuration

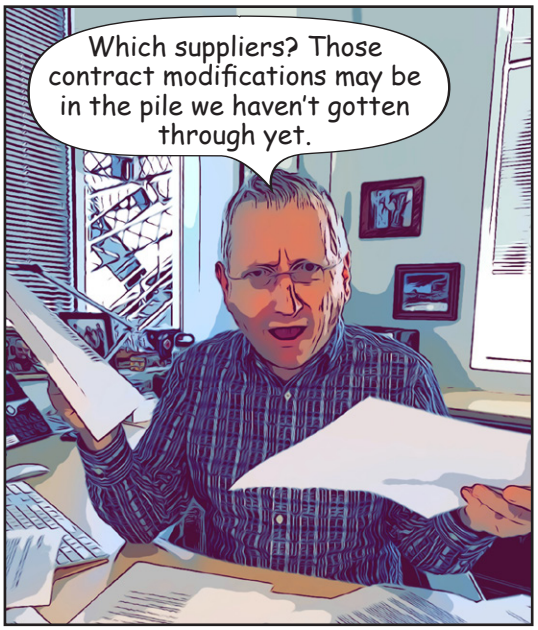
35 high
42 med



It wouldn't have been such a terrible day if...

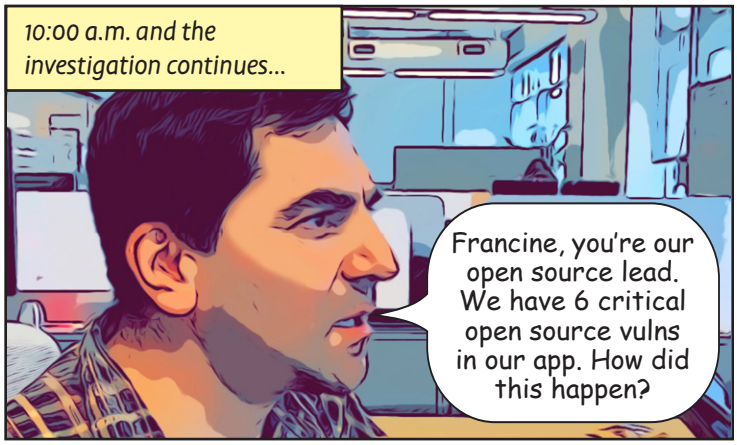
The organization had integrated AppSec training into the developers' workflow so they could learn as they coded.

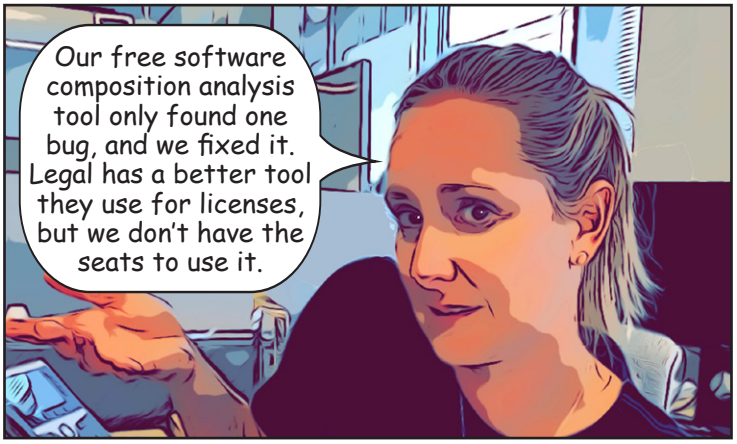

At 9:30 a.m. Alex pays a visit to the legal department.
We found 5 critical vulns in code from our suppliers. Don't they have to give us secure code?

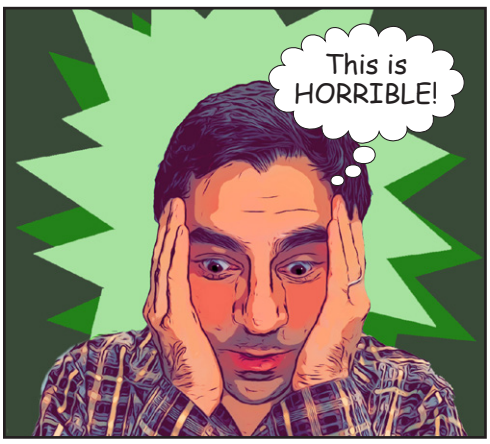

Which suppliers? Those contract modifications may be in the pile we haven't gotten through yet.

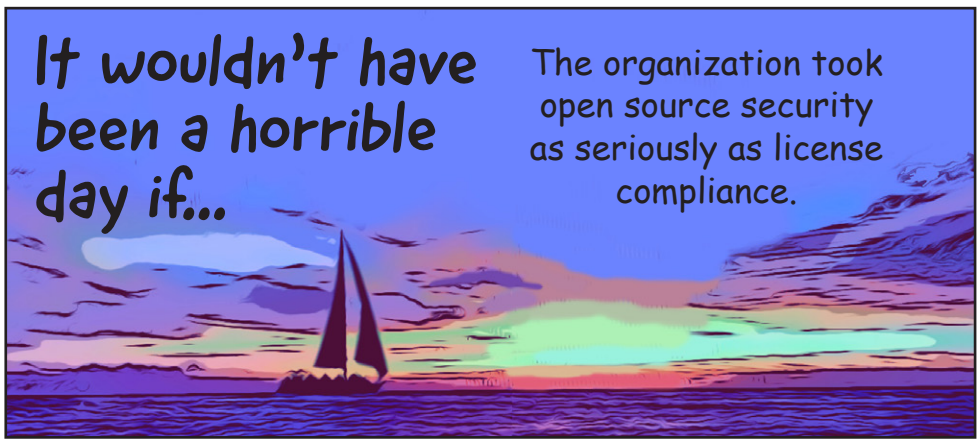

This is NO GOOD!

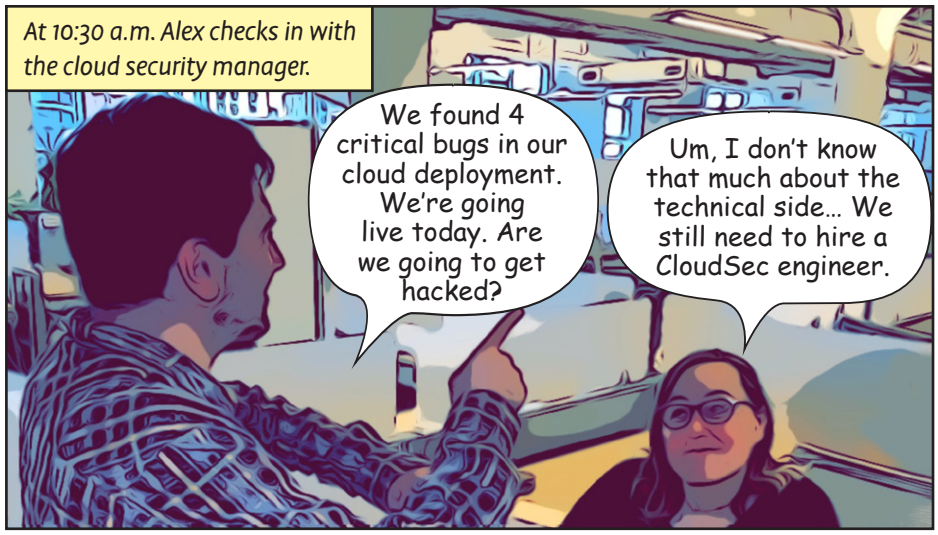

It wouldn't have been such a NO GOOD day if...
The organization had included Legal and Procurement in the buying decision for third-party software so they could manage the risks.

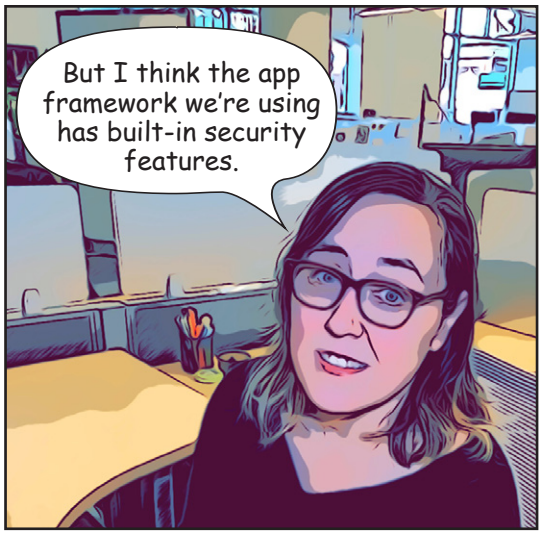

10:00 a.m. and the investigation continues...
Francine, you're our open source lead. We have 6 critical open source vulns in our app. How did this happen?


Our free software composition analysis tool only found one bug, and we fixed it. Legal has a better tool they use for licenses, but we don't have the seats to use it.


This is HORRIBLE!

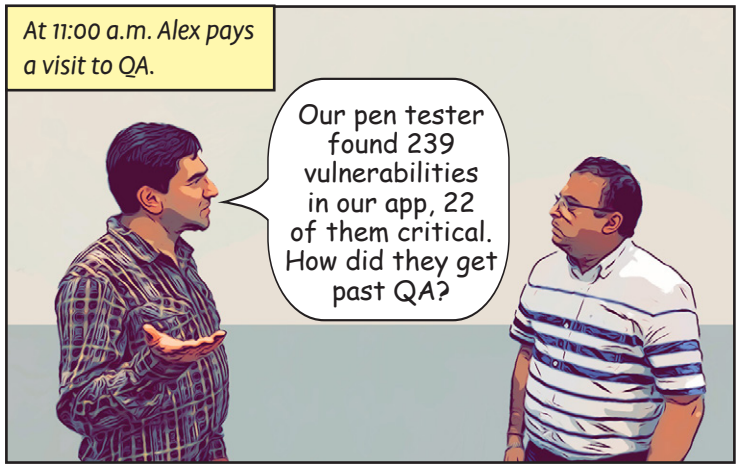

It wouldn't have been a horrible day if...
The organization took open source security as seriously as license compliance.


At 10:30 a.m. Alex checks in with the cloud security manager.
We found 4 critical bugs in our cloud deployment. We're going live today. Are we going to get hacked?
Um, I don't know that much about the technical side... We still need to hire a CloudSec engineer.


But I think the app framework we're using has built-in security features.


But framework isn't design.
This is VERY BAD!


It wouldn't have been a VERY BAD day if...
The cloud security team really understood the difference between security software and software security.


At 11:00 a.m. Alex pays a visit to QA.
Our pen tester found 239 vulnerabilities in our app, 22 of them critical. How did they get past QA?

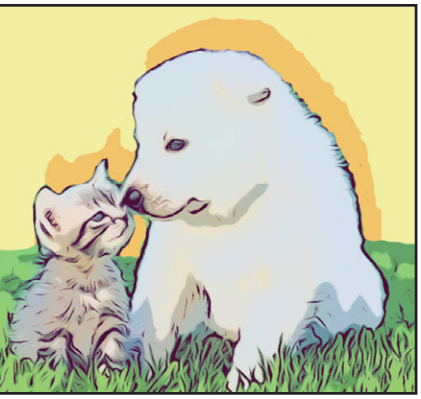

We don't QA for security bugs. We'd never hit our deadlines if we did.
But going back to fix these bugs takes even more time.


Not my problem.


This is very bad!!
We can't go live with 22 critical vulnerabilities.

It wouldn't have been such a VERY BAD day if...

QA had used interactive application security testing, which finds quality AND security issues.



It's noon.

Is the app ready to go? I'm going to demo it live at our launch party.

I don't know if that's a good idea. The app's full of issues we can't possibly fix in time.

Well, everything is in motion. We've spent millions on this launch party. so it has to be ready. You'll just have to push it to production as is.

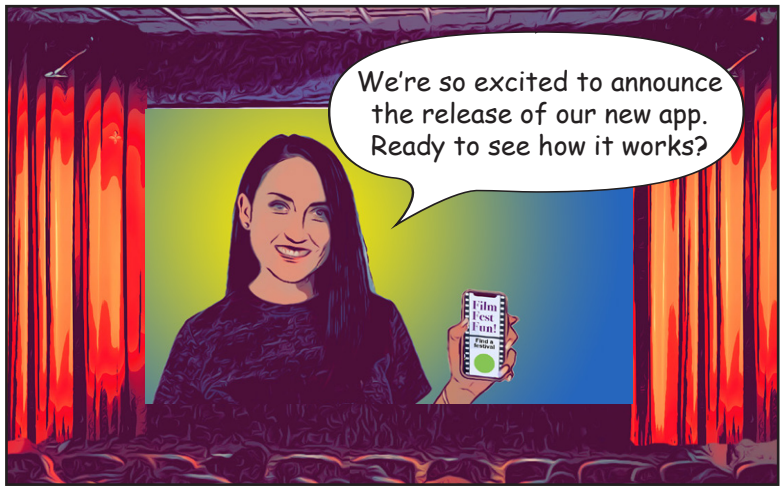
This is VERY VERY BAD!

It wouldn't have been a VERY BAD day if...

The organization had built testing into the development cycle from start to finish so they didn't get buried under vulnerabilities at the end.

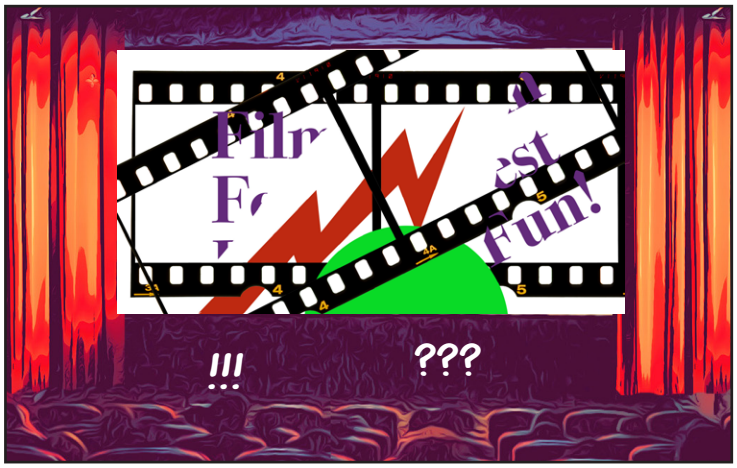
At 6:30 p.m. the doors of the local theater open for the launch party.

FILMFESTFUN
APP LAUNCH PARTY

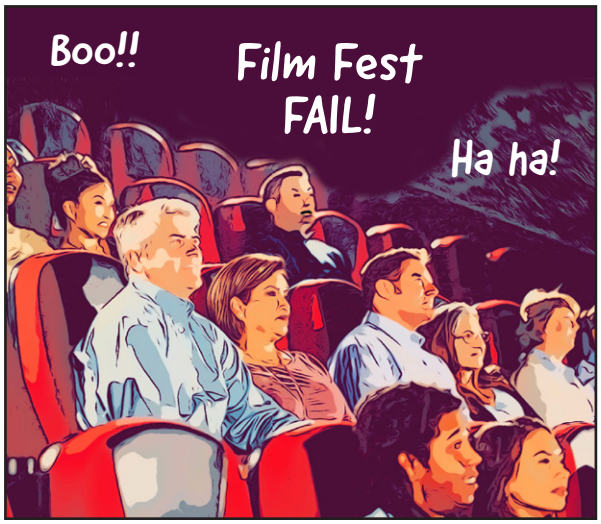

We're so excited to announce the release of our new app. Ready to see how it works?
Film Fest Fun!
Find a festival


Woo!!
Yes!!
Yay!


Film Fest Fun!
Find a festival
Go


!!!
???


YOU'VE BEEN HACKED!!


Boo!!
Film Fest FAIL!
Ha ha!


And so the curtain falls on Alex's job at FilmFestFun.
LinkedIn

HOW TO HAVE A WONDERFUL, AMAZING, NOT BAD, VERY GOOD DAY!

Integrate AppSec training into your developers' workflow so they can learn as they code– with **Polaris with Code Sight**. Code Sight gives developers vulnerability remediation guidance as they code with eLearning integrated into the IDE.

Include Legal and Procurement in buying decisions for third-party software so they can manage the risks. Synopsys **Security Strategy and Planning Services** assess the maturity of your software security initiative and deliver a plan to close gaps and address your risk management goals.

Take open source security as seriously as license compliance. **Black Duck** gives you visibility and control of open source for security and license risks throughout the SDLC.

Understand the difference between security software and software security. With **Threat Modeling** and **Architecture Risk Analysis**, you can identify weaknesses and address security early in the SDLC to reduce attack susceptibility and avoid costly rework.

QA should use interactive application security testing tools, which find quality AND security issues. **Seeker** continuously monitors application testing and provides immediate auto-verified results.

Build testing into the development cycle from start to finish with the **Synopsys Software Integrity Portfolio** so you don't get buried under vulnerabilities at the end. Synopsys helps your security and development teams build secure, high-quality software faster.

If you try to solve your application security problems one at a time, you're not improving. It's time to do something different. Synopsys provides the only solution that has all the tools and services you need to help build or mature a complete software security solution efficiently: soup to nuts.

THE SYNOPSYS DIFFERENCE

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

06/20/19.TheCISOsTerribleNoGood-final.