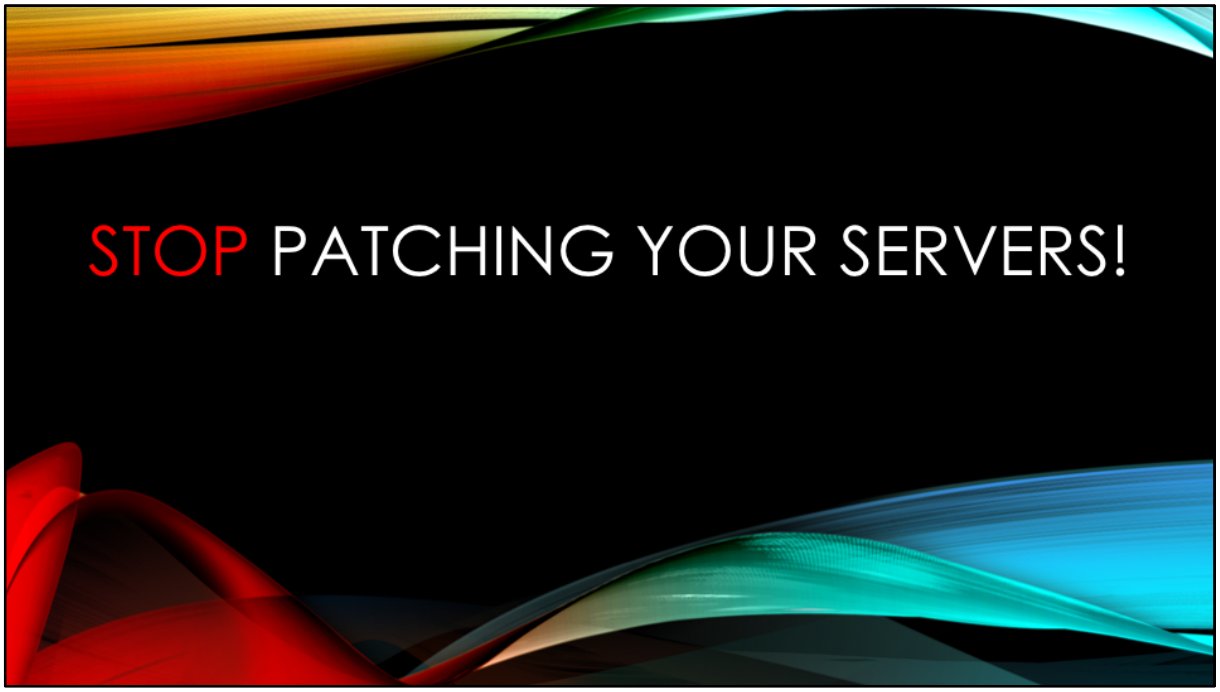
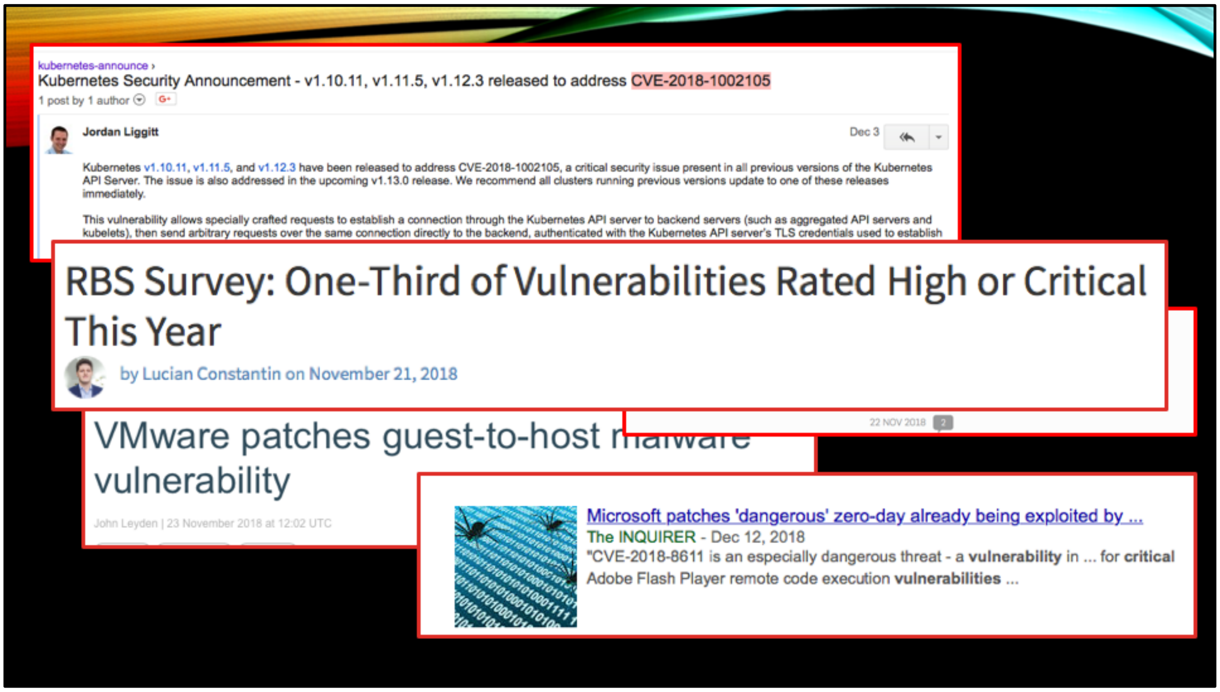


STOP PATCHING YOUR SERVERS!

Get your attention?



kubernetes-announce ›

Kubernetes Security Announcement - v1.10.11, v1.11.5, v1.12.3 released to address CVE-2018-1002105

1 post by 1 author

Jordan Liggitt

Dec 3

Kubernetes v1.10.11, v1.11.5, and v1.12.3 have been released to address CVE-2018-1002105, a critical security issue present in all previous versions of the Kubernetes API Server. The issue is also addressed in the upcoming v1.13.0 release. We recommend all clusters running previous versions update to one of these releases immediately.

This vulnerability allows specially crafted requests to establish a connection through the Kubernetes API server to backend servers (such as aggregated API servers and kubelets), then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish

RBS Survey: One-Third of Vulnerabilities Rated High or Critical This Year

by Lucian Constantin on November 21, 2018

22 NOV 2018

VMware patches guest-to-host malware vulnerability

John Leyden | 23 November 2018 at 12:02 UTC

Microsoft patches 'dangerous' zero-day already being exploited by ...

The INQUIRER - Dec 12, 2018

"CVE-2018-8611 is an especially dangerous threat - a **vulnerability** in ... for **critical** Adobe Flash Player remote code execution **vulnerabilities** ...

Kubernetes patch…. VMWare …. Flash….

How many worked on this and drove it’s remediation?

Raise Hand?

Comment on response - Everyone? Half? No one?

We’ve all seen these types of responses and been directly involved in mitigating risk.

I know I feel like this in my role.

For those that don’t know me, I’m Joe Tegg.

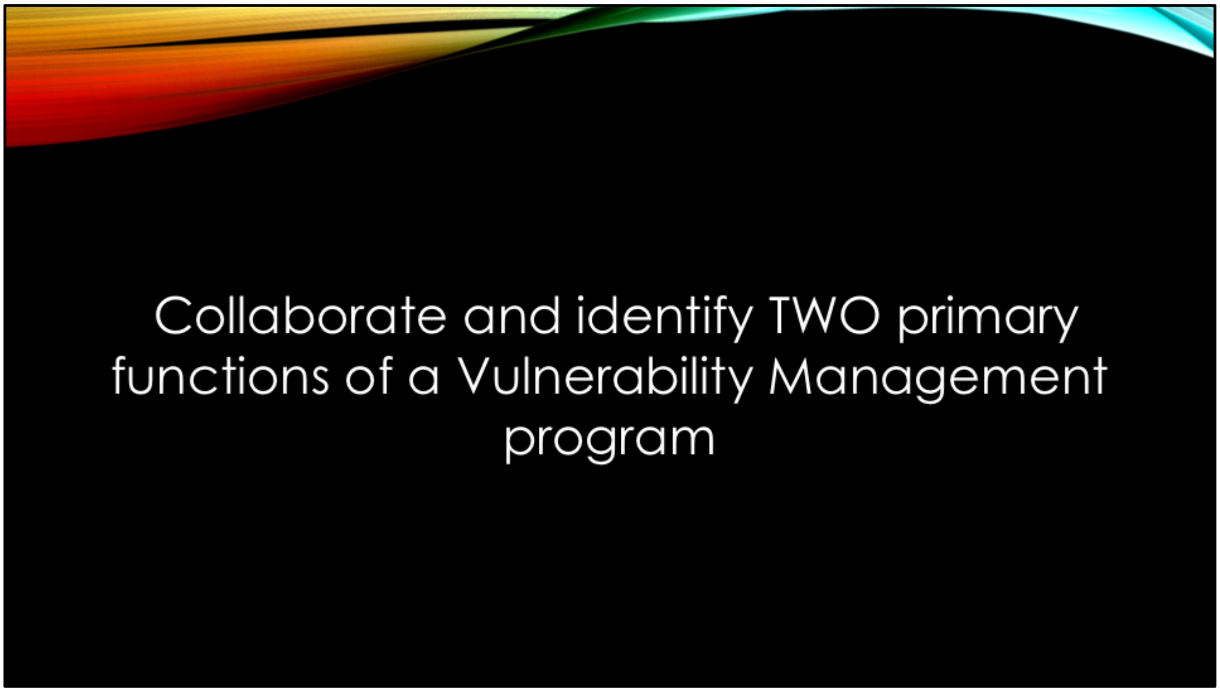
I’m a Vuln Management zealot
Question asker
Bear poker

And some of you know me as a chicken farmer

This is how Vuln Management looks in many companies, big and small.

You can have a team of 10 all the way down to a single person, and I bet they’d all say they feel like this a lot of the time.

Imagine if we could stop doing this and work towards something more effective…



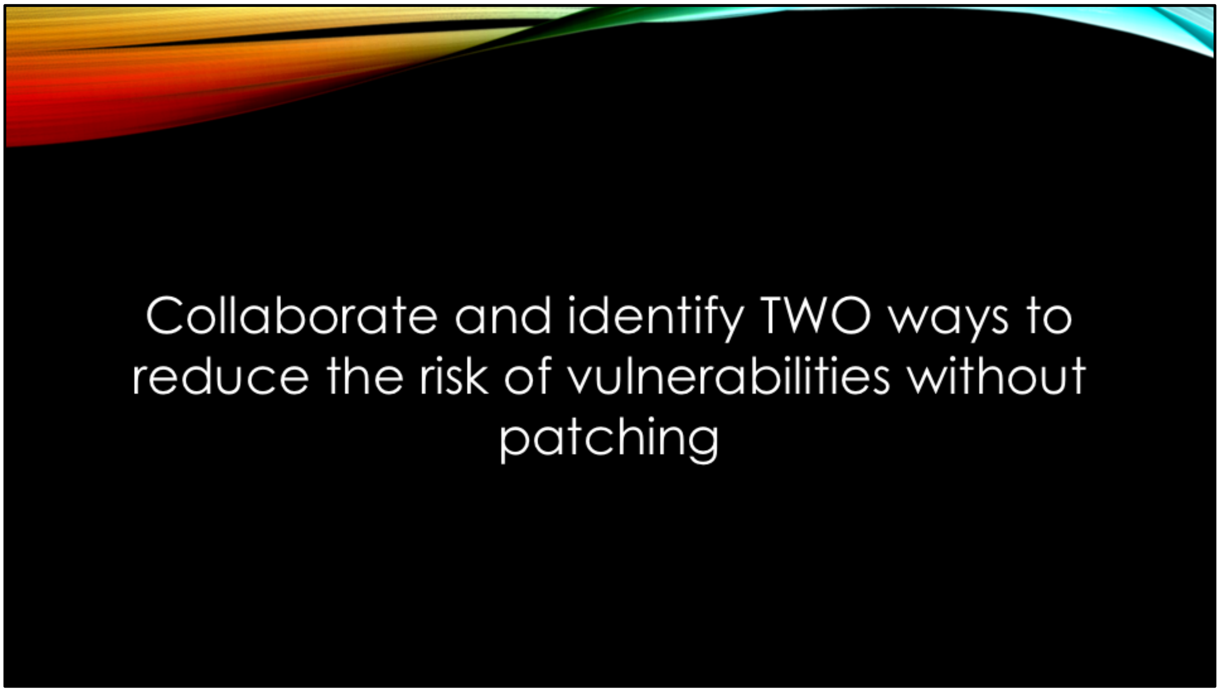
Collaborate and identify TWO primary functions of a Vulnerability Management program

Break them into groups and tell them what we expect – Start at the back and go around to each group

Drive them to converse by saying “the one in each group that’s been at their job the longest, writes the first answer”

--

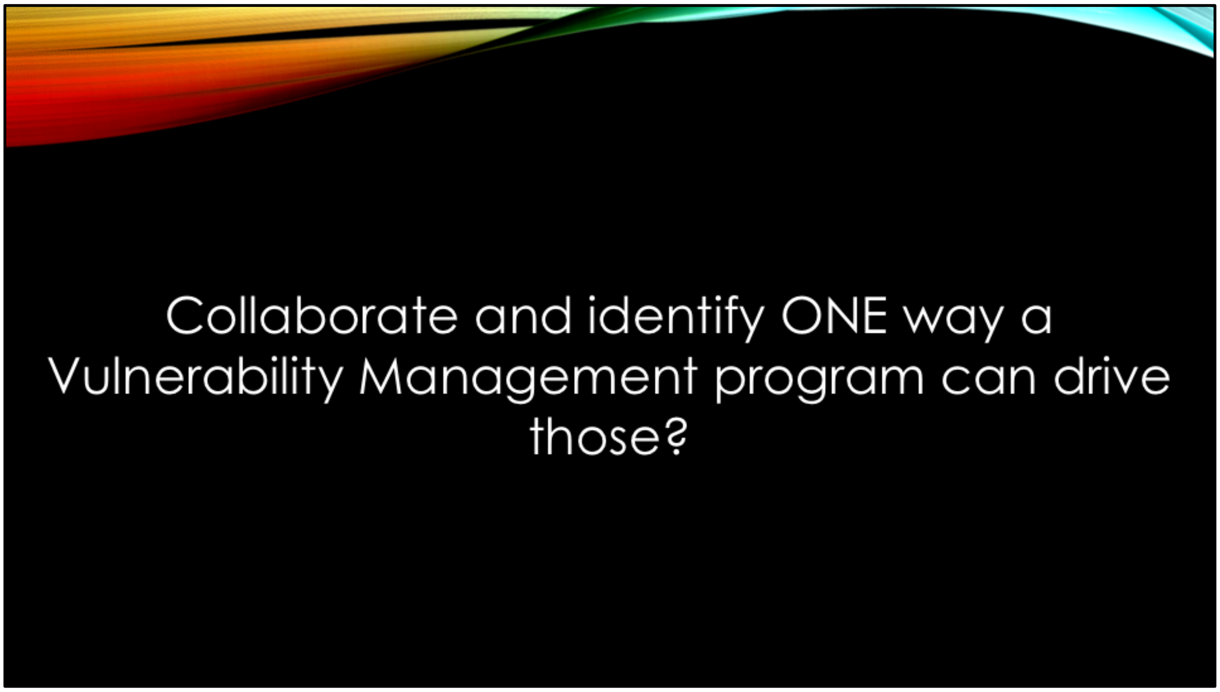
- Drive patching programs?
- Provide Patch related Operational Reporting?
- Provide Patch related KPI Reporting?
- Provide Consulting on remediation plans?
- Provide Consulting on exception requests?



Collaborate and identify TWO ways to reduce the risk of vulnerabilities without patching

There is more to vulnerability management than patching

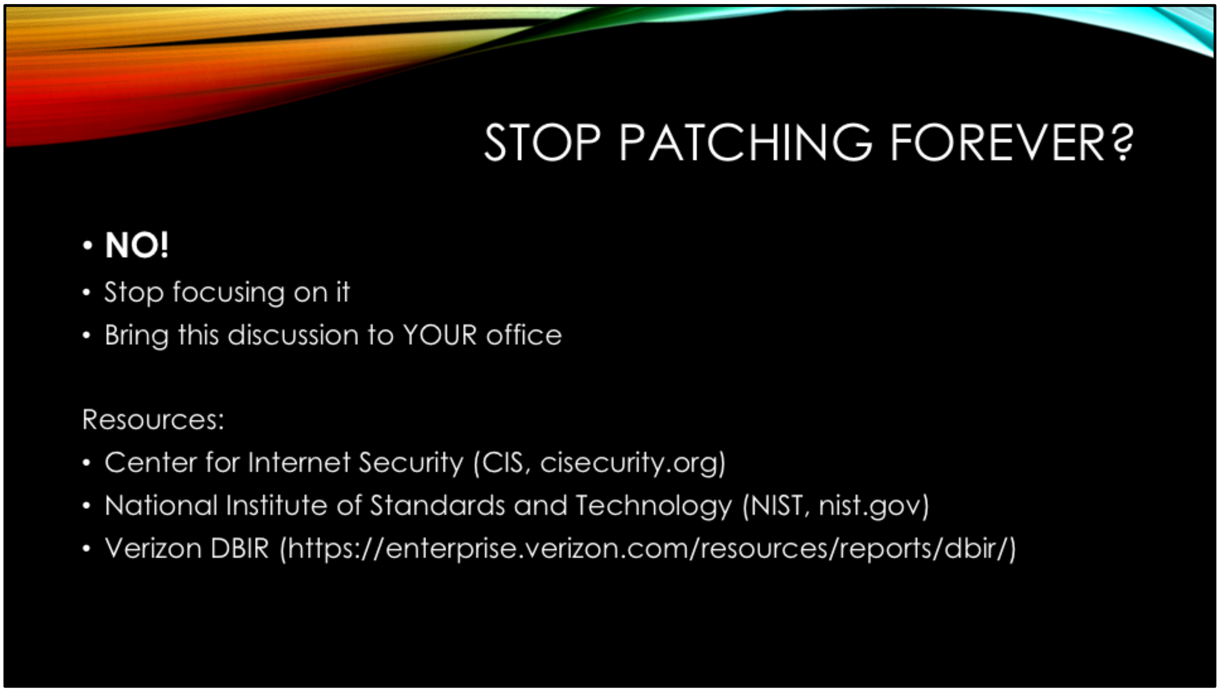
1. Secure Baselines / OS Images
2. Configuration Management
3. FW / IDS Rules? – Plug into SecOps
4. Security Awareness – Teach Ops teams to be mindful of security before it becomes a request



Collaborate and identify ONE way a Vulnerability Management program can drive those?

Drive strategic changes in the risk management of the Operational teams?

- Consulting - Drive Secure Baseline Images
- Consulting - Drive Secure Configuration Management
- Consulting – Drive Control Management/Verification (FW, IPS, IDS, Honey*) – SecOps, Security Architecture
- Reporting – Use Strategic KPIs and executive reporting



STOP PATCHING FOREVER?

- **NO!**
- Stop focusing on it
- Bring this discussion to YOUR office

Resources:

- Center for Internet Security (CIS, cisecurity.org)
- National Institute of Standards and Technology (NIST, nist.gov)
- Verizon DBIR (https://enterprise.verizon.com/resources/reports/dbir/)

Am I telling you to stop patching completely?

No

I was just asking questions to help all of us think about the other things that can be a force multiplier for VM teams

Wrap up –

I hope you were able to gain some new perspective or ideas from our discussion and questions.

Maybe together we can drive Vulnerability Management to feel more like this happy and confident dam engineer during the next critical vulnerability announcement.