Guerrilla GRC

Let’s streamline vendor assessments

ACoD 2020 - Austin, TX - 15 Jan 2020

yubico

$ whoami

John Duksta

- Principal Security Engineer @ Yubico
- Previously @ Amazon, Secureworks, Verisign, BBN

Areas of focus

- Infrastructure Security (traditional and cloud)
- Zero Trust
- Applied Cryptography

@ducksauz

yubico

Being Cloud Native

Photo credit: Joe Mabel - CC BY-SA 4.0

yubico

Most every tool is a vendor

$HRIS

$CRM

$STORAGE

$EXPENSING

$ALERT_MANAGER

$CLOUD

$VIDEO_CONFERENCE

$RECRUITING

$SRC_MGMT

$SERVICE_DESK

$GRAPHICS

$TRAVEL

$LOG_MGMT

$ERP

$MARKETING_THING

$PLM

By the numbers

~250 employees

5 security engineers + 1 TPM + 1 CISO

0 GRC people

45 outbound vendor security assessments

8 inbound vendor security assessments

On average, 1 assessment per week in 2019

I want it all, and I want it now!

yubico

Process

- Get request
- Determine data classification involved
- Calibrate review accordingly
- Collect and review data
- Write report and make recommendation

Variable Speed

Tier 1

- Most sensitive data
- Critical service
- Potential for irreparable harm
- ~16-32 person hours
- 3-4 weeks

Tier 2

- Non-sensitive data
- Non-critical service
- ~8-16 person hours
- ~2 weeks

Tier 3

- Usually public data
- ~3-4 person hours
- ~1 weeks

Document Review

Policy Documents

Pentest Report

Non Invasive Tech Review

- Mozilla Observatory/SSL Labs
- Federated Login Support
- Logging/Audit Support

Other bits

- Historical security incidents
- Do they have a /security page
- Do they have a security@ alias

Report and Advise

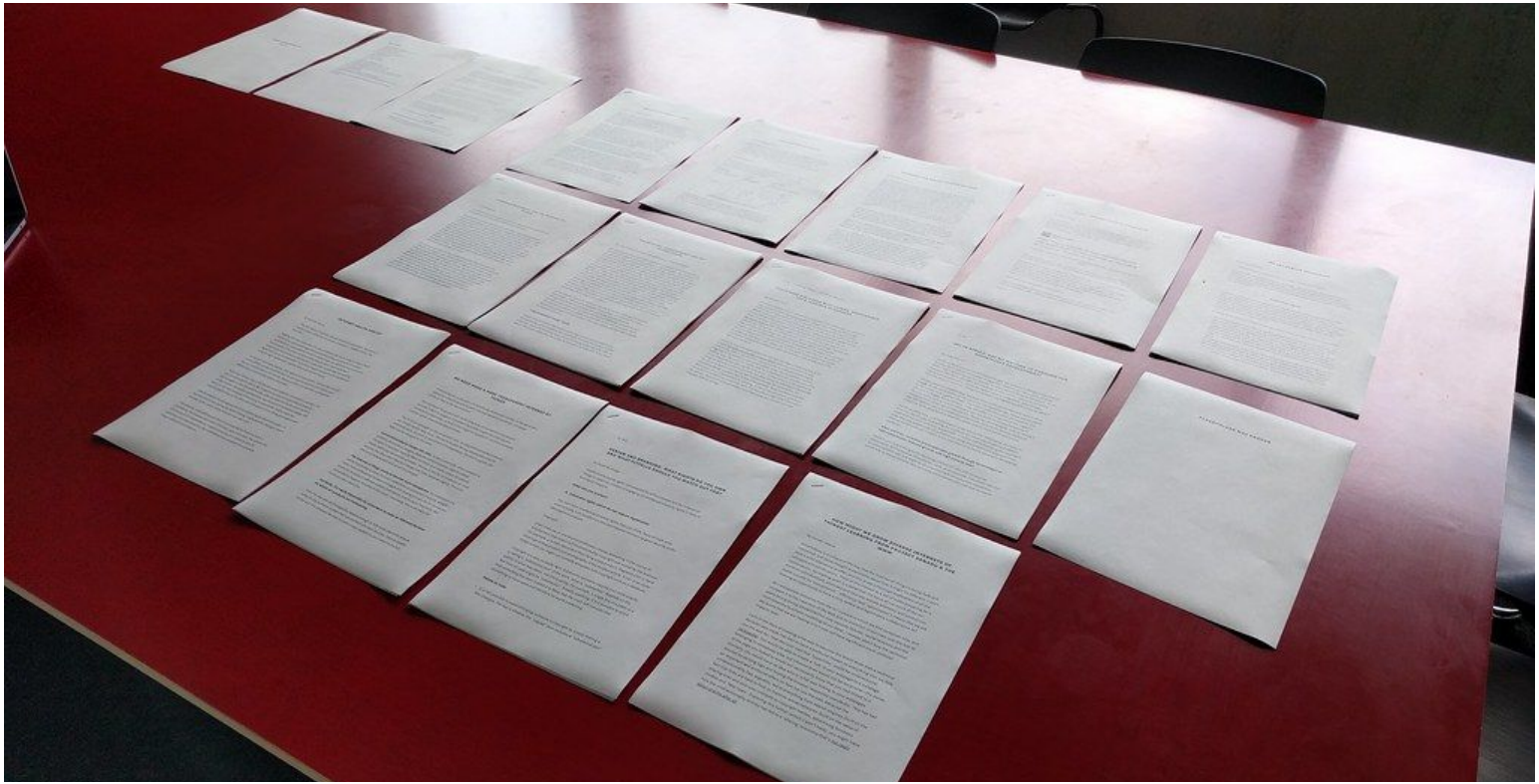

Image by: waving cat -CC BY-NC-SA 2.0

Can we make this better?

What are you doing?

Is this faster or slower for you?

Let’s talk about the process and build some guidance.

Oblig: We're Hiring

Product Security Engineer

- **Bellevue, WA and Stockholm, SE**

Security Assurance (GRC) Manager

- **Bellevue, WA or Stockholm, SE**

Talk to me, or email me: jccd@yubico.com

yubico