Incident Response *for Devs*

Tanya Janca

And DevOps Folks Too!

IR For Everyone!

Tanya Janca

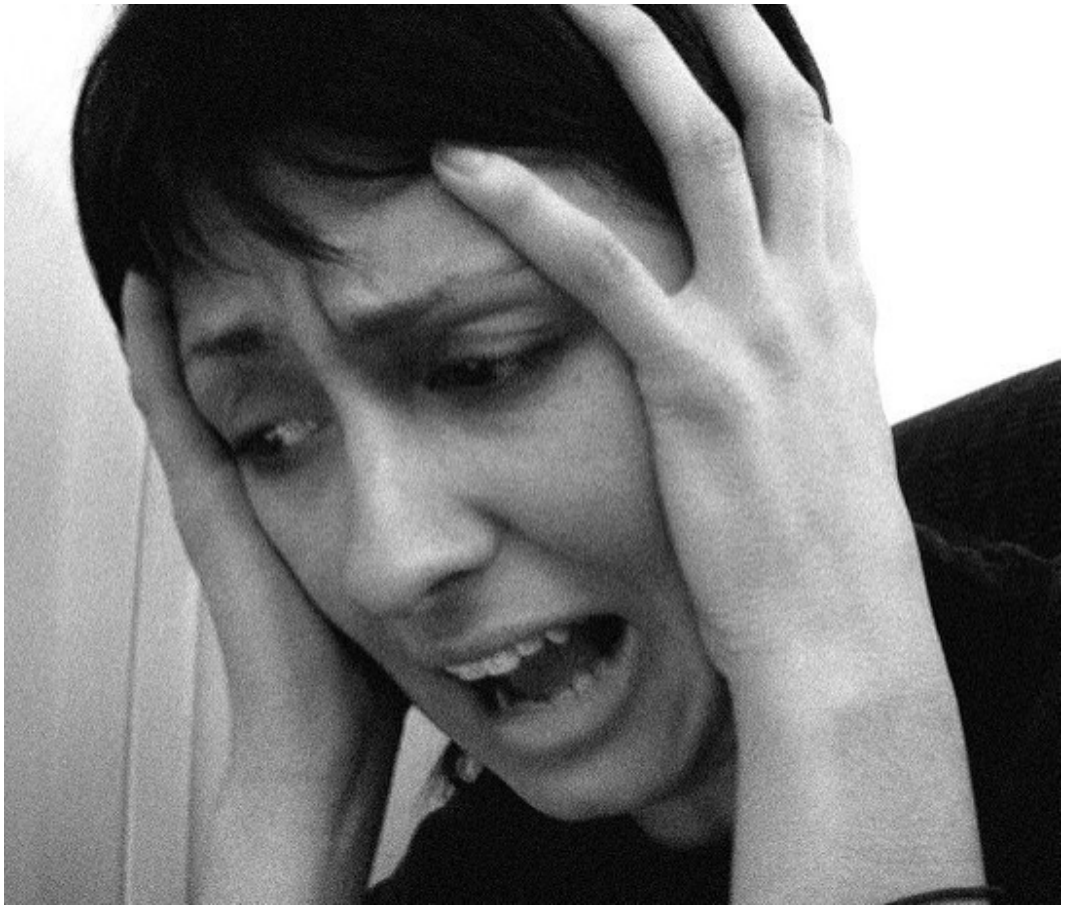
- Head of Community and Education at Semgrep!
- Founder @ We Hack Purple
- AKA @SheHacksPurple
- Author: **Alice and Bob Learn Application Security**
- 25+ years in tech, Sec + Dev
- Advisor: Cloud Defense, Nord, Aiya Corp
- OWASP Chapter and Project founder
- Blogger, Podcaster, Streamer, Builder, Breaker
- Nerd at Large

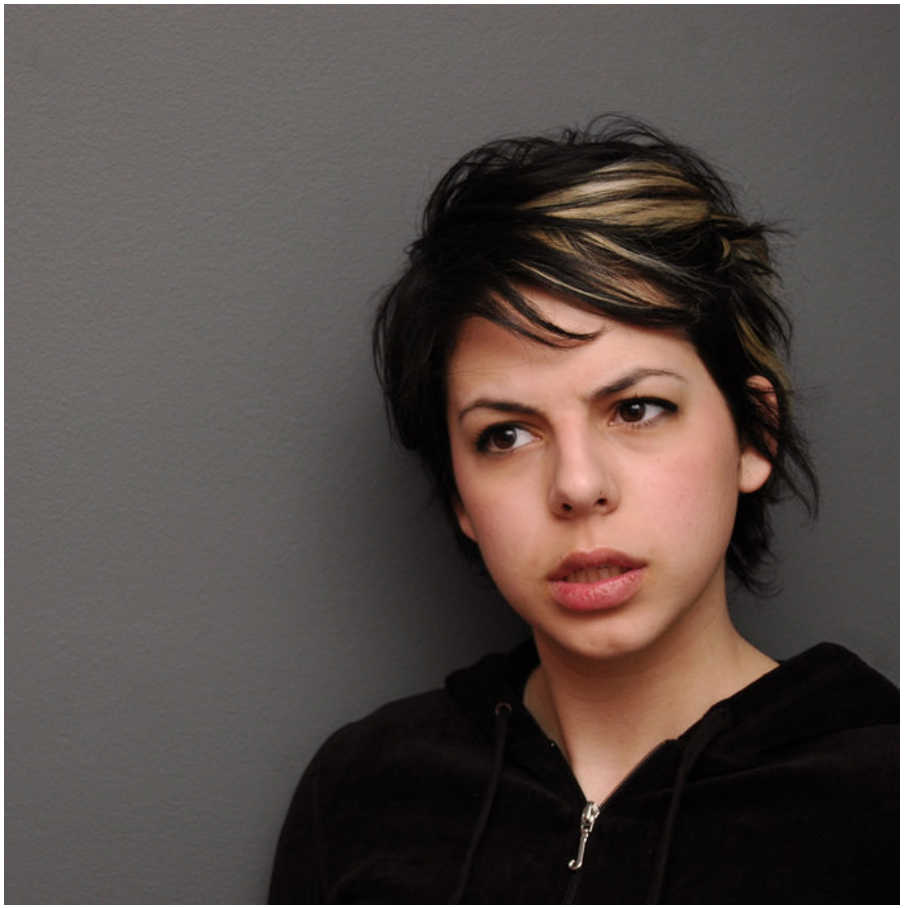
What is Incident Response?

An organized approach to addressing and managing the aftermath of a security breach or IT **incident**. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

http://searchsecurity.techtarget.com/definition/incident-response

Security Incident or Event?





Security Incident or Event?

In simple terms:

A security event is when something strange has happened or you suspect something is wrong.

A security incident is when you are certain something bad has or is happening.

Example; you find your data for sale on the dark web. THAT is an incident!

Trigger Warning

I’m going to tell one story where something very bad happens. To children. It will not be graphic, but please leave if you need to.

Your org needs its apps secured.

Devs are the first line of defense for apps.

Without your buy-in, we're lost.

If something happens, sometimes we need your help.

#WOCTECHCHAT

@SheHacksPurple

Security Incidents

Your Role, ‘Need To Know’, and Stories.

Your Role During an Incident

1. Tell the security team if you see something. It's better to report something and be wrong than to have it the other way around.

Photo by Joshua J. Cotten on Unsplash

Your Role During an Incident

2. Don’t leave the premises without telling them!

Photo by Johen Redman on Unsplash

Your Role During an Incident

3. This is top priority, treat it like the emergency it is.

Photo by camilo jimenez on Unsplash

Your Role During an Incident

4. Follow “need to know”.

Photo by Kristina Flour on Unsplash

Your Role During an Incident

5. Do not try to manage it yourself and ‘be a hero’.

Photo by Clark Van Der Beken on Unsplash

Picture Slide!

Your Role During an Incident

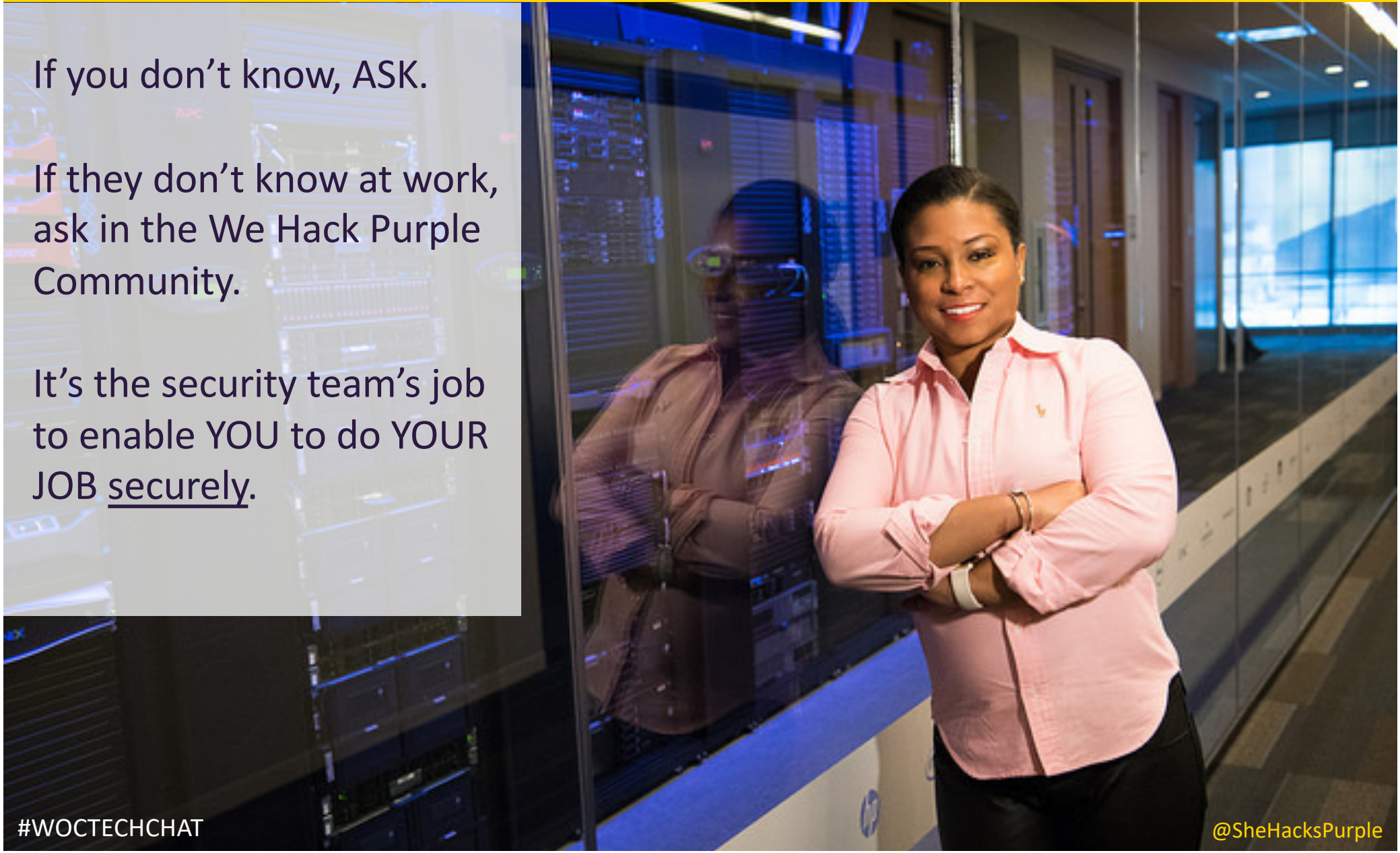
1. Tell the security team if you see something. It's better to report something and be wrong than to have it the other way around.
2. Don't leave the premises without telling them!
3. This is top priority, treat it like the emergency it is.
4. Follow "need to know".
5. Do not try to manage it yourself and 'be a hero'.

Talk to the AppSec Team!

If you don't know, ASK.

If they don't know at work, ask in the We Hack Purple Community.

It's the security team's job to enable YOU to do YOUR JOB securely.



#WOCTECHCHAT

@SheHacksPurple

Resources

Awesome Books

- The DevOps Handbook
- The Phoenix Project
- Accelerate
- The Unicorn Project
- Alice and Bob Learn Application Security

#CyberMentoringMonday

Every Monday!

We Hack Purple Community

The We Hack Purple community is a fun and safe place to learn all things security. Join us to learn about AppSec, DevSecOps, cloud and more.

Network, learn and (hopefully) make new friends!

https://Community.WeHackPurple.com

Join the Semgrep community!!!!!

https://bit.ly/semgrepnewsletter

https://bit.ly/semgrepslack

https://bit.ly/trysemgrep

Resources: ME!!!!

Twitter: @SheHacksPurple

https://SheHacksPurple.ca/blog

https://YouTube.com/SheHacksPurple

https://NewsLetter.SheHacksPurple.ca

https://infosec.exchange/@SheHacksPurple

THANK YOU!

Tanya Janca

SheHacksPurple