Being the first dedicated security hire and growing a team.

Mike Sheward

@secureowl@infosec.exchange

```
{o,o}
|)__)
_"_"_
```

SUM 41
All Killer No Filler

whoami

Currently Head of Security @ Xeal = EV Charging

Originally from the U.K, but done a Brexit before it was cool

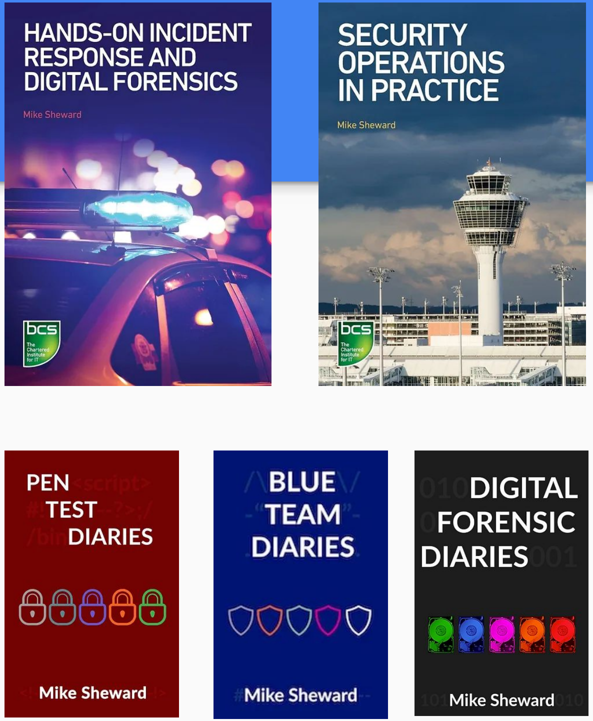
~18 years in InfoSec, mostly Blue Team in US

Built SaaS and Platform security teams

Written some books ->

Avid shitposter: @secureowl@infosec.exchange

```
{o,o}
|)___)
_"_"_
```


HANDS-ON INCIDENT RESPONSE AND DIGITAL FORENSICS
Mike Sheward
bcs The Chartered Institute for IT
SECURITY OPERATIONS IN PRACTICE
Mike Sheward
bcs The Chartered Institute for IT
PEN TEST DIARIES
Mike Sheward
BLUE TEAM DIARIES
Mike Sheward
DIGITAL FORENSIC DIARIES
Mike Sheward

infosecdiaries.com + Amazon + Audible + Book Stores + Walmart

First dedicated security hire?

What you might find, and why Sum 41's Album is so important in determining your security scenario

- All Killer No Filler
- No Killer All Filler
- Some Killer Some Filler
- No Killer No Filler

1) All Killer No Filler

1) All Killer No Filler

How to recognize?

Typically engineering driven/led security programs.

Some good ‘pockets’ of controls in place, doesn’t always cover entire business.

Can be identified by randomly deployed fancy tools without a surrounding strategy.

What to do with it?

Be the filler! Join those pockets together.

Don’t buy new tools, make the most of what you have.

Focus on policies and applying the engineering elements to the rest of the business.

1) All Killer No Filler

Real example: Having a bug bounty program before a security program

- Bug bounties are often seen as a sign of operational security maturity.
- Yes, they can be valuable - but they can also be a distraction.
- Have a vulnerability management program before a bug bounty.

Lesson learned: Purge the backlog, close down or scope the program, and build the mechanisms for internal vulnerability discovery first.

First hire: entry-mid level analyst OR maybe bring that person in from engineering.

2) No Killer All Filler

2) No Killer All Filler

How to recognize?

Typically legal/finance driven programs.

Lots of documentation, including policies, but not much enforcement or monitoring.

May have some tools, but typically not fully deployed.

What to do with it?

Read the policies, read the docs, and figure out how much of it aligns with business goals.

Look at your tools, finish deploying the ones you have if they make sense.

Ask the engineering/IT teams what they have in place that you can reuse - make it killer!

2) No Killer All Filler

Real example: People didn’t know there was a security policy, it was kept hidden

- IT and engineering we’re among the most excited someone was around to actually write a security policy.
- Thing is, there had been one, very boilerplate-y policy around for years.
- No one had attempted to put that policy into action.

Lesson learned: Never underestimate the power of talking to people. Most people want guidelines and to know how to do thing the correct way, they just won’t ‘seek it out’, because they have jobs.

First hire: Application Security engineer to solidify relationship with eng.

3) Some Killer Some Filler

3) Some Killer Some Filler

How to recognize?

No ‘true’ pre-existing security program in place, likely just bits and pieces that have been done to meet customer needs.

Controls may have originated in IT.

Could be a history of ‘false starts’ and shifting ownership of security.

What to do with it?

Inventory what you have.

Look for clues about what should be your priority - what have customers asked about previous?

Alternate between building the killer and the filler.

Identify who has been involved in previous iterations.

3) Some Killer Some Filler

Real example: No one talked about the 'killer'

- The policy said one thing, the reality was another - but in a good way!!
- Engineering had built some pretty good processes and systems, but didn't know how to publicise them.

Lesson learned: People not in security can be nervous about, or simply not realize the value in what they are doing from the security perspective - help them promote it internally and externally.

First hire: Engineer focused on control deployment.

4) No Killer No Filler

4) No Killer No Filler

How to recognize?

There is literally nothing.

Like nothing.

Hopefully you’re at an early stage startup.

“Well we’re in AWS, so that gives us security, right?”

What to do with it?

Talk to the people.

Ask the business peoples what is the most significant risk to the business.

Ask about compliance needs and customers requirements.

Inventory your assets.

Buckle up.

4) No Killer No Filler

Real example: Launching with a massive security and productivity enabler

- Zero controls in place, so started with SSO.
- SSO is a security tool in disguise.
- SSO illuminates shadow IT.

Lesson learned: People love SSO, it is used everywhere and can be one of the greatest sources of intelligence you'll ever have.

First hire: generic senior security engineer.

In conclusion

- You’re in for an awesome experience
- Learn as much as you can
- You will have good days and bad days
- You will question your ability to do the thing (you can do it of course)
- Don’t let it impact your health
- Always remember businesses are not in business to be secure (add value beyond security)
- Technical and non-technical things are needed, so there is room for anyone from any background
- And most importantly: sometimes places lie
    - There were at most four ‘killer’ tracks on All Killer No Filler

```
{o,o}
|)__)
_"_"_
```

Thank you! Let’s stay in touch

#INFOSEC!
0DIARIES1

@secureowl@infosec.exchange

infosecdiaries.com

linkedin.com/in/mikesheward/