BlackHat Squirrel

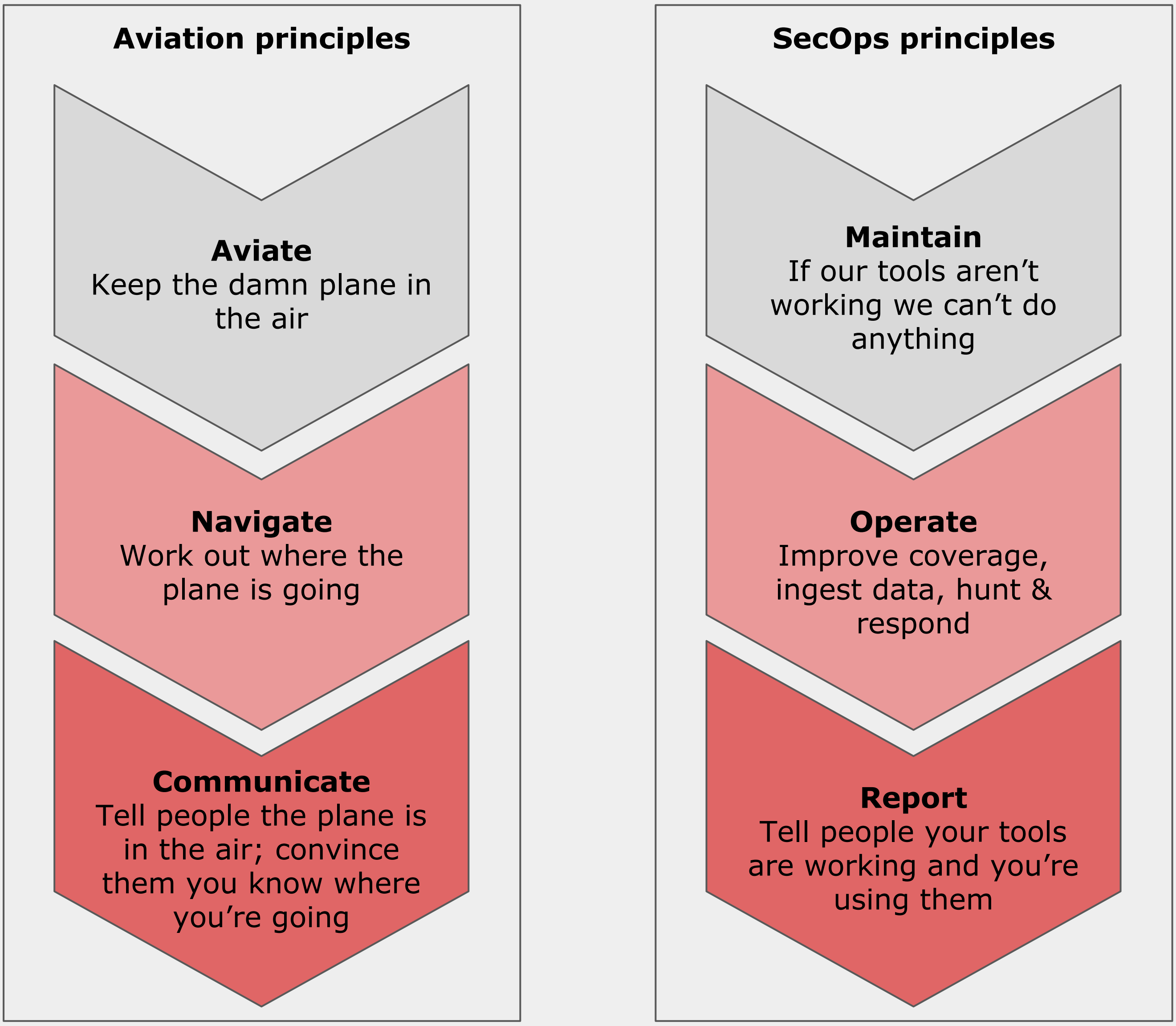
https://github.com/blackhatsquirrel

SecOps Management

Because running SOC is like flying a plane

Running an efficient and effective SecOps team is arguably the hardest job in IT, let alone security. We’re all really excited about plugging in sexy new boxes with flashy lights but when it comes to actually running the damn things we’re at a loss. Even approaching what you’re meant to do is a nightmare. Does it include patching? Are we a hunt team? Is it more than just a SOC? These are all questions which you’ve no doubt ignored in the interest of avoiding as much work as possible. Fortunately we’ve come up with a very straightforward way of explaining to your boss what you’re meant to do. Whether or not what you’re meant to do is what you’re actually doing is another story…

A few years ago we were told by a pilot friend of ours about the three principles of aviation. Several thousand beers later we decided this probably isn’t a bad way of looking at security operations.



Aviation principles

Aviate
Keep the damn plane in the air

Navigate
Work out where the plane is going

Communicate
Tell people the plane is in the air; convince them you know where you’re going

SecOps principles

Maintain
If our tools aren’t working we can’t do anything

Operate
Improve coverage, ingest data, hunt & respond

Report
Tell people your tools are working and you’re using them

Aviate

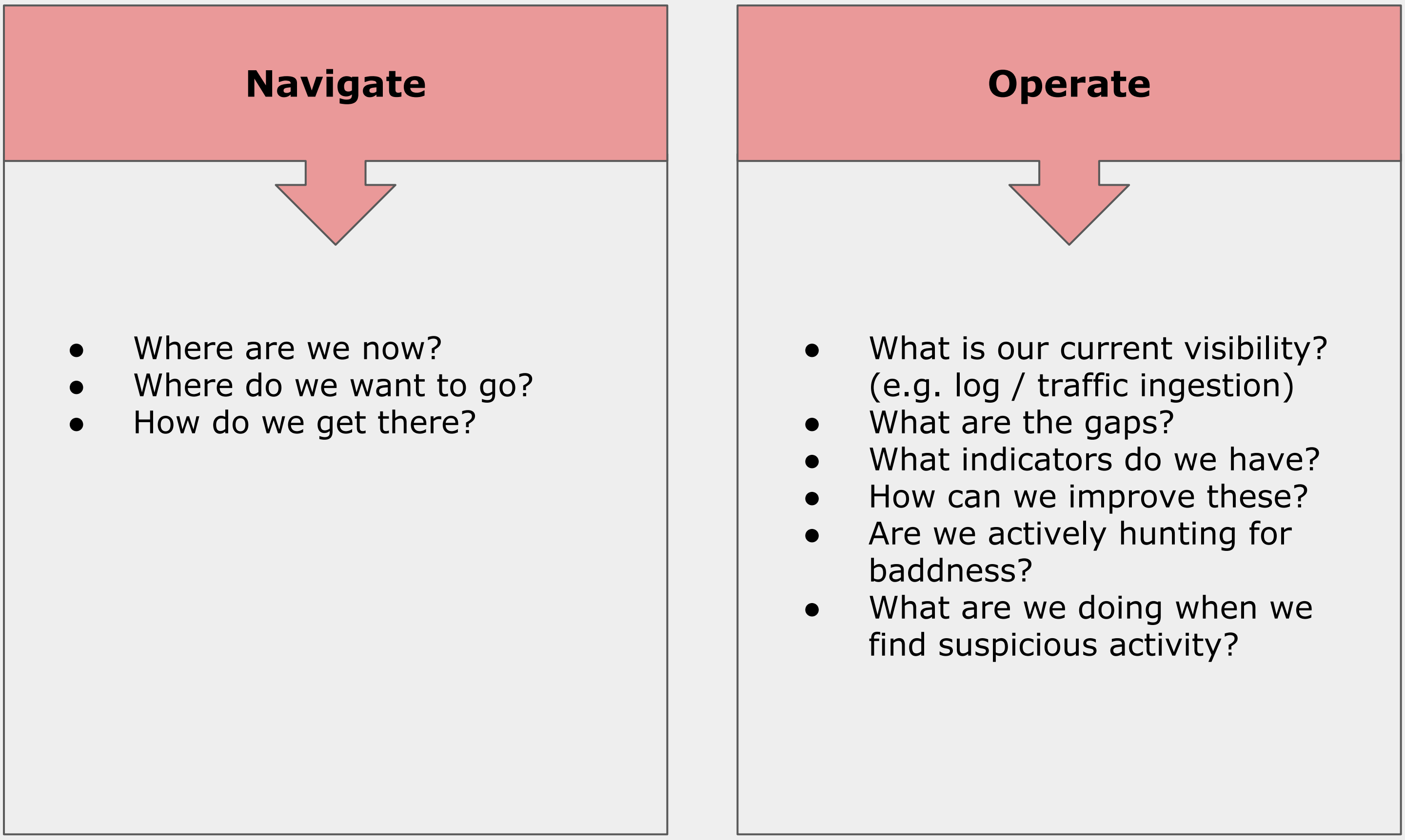
- Are you currently in the air?
- Are the engines making noises?
- Is anything on fire?
- Are there lots of red lights flashing on the dashboard?
- Does the level thing make the plane move still?

Maintain

- Do you have access to all your systems?
- Do you even know where they are?
- Are you monitoring their performance?
- Have you assessed the capacity?
- Do you even know their capacity?
- Do you know how to fix them when they go wrong?
- Do you have contacts at your suppliers?

BlackHat
Squirrel

https://github.com/blackhatsquirrel



Navigate

- Where are we now?
- Where do we want to go?
- How do we get there?

Operate

- What is our current visibility? (e.g. log / traffic ingestion)
- What are the gaps?
- What indicators do we have?
- How can we improve these?
- Are we actively hunting for baddness?
- What are we doing when we find suspicious activity?

Communicate

- Who do we need to speak to?
- What do we need to tell them?
- What information do we need in return?

Report

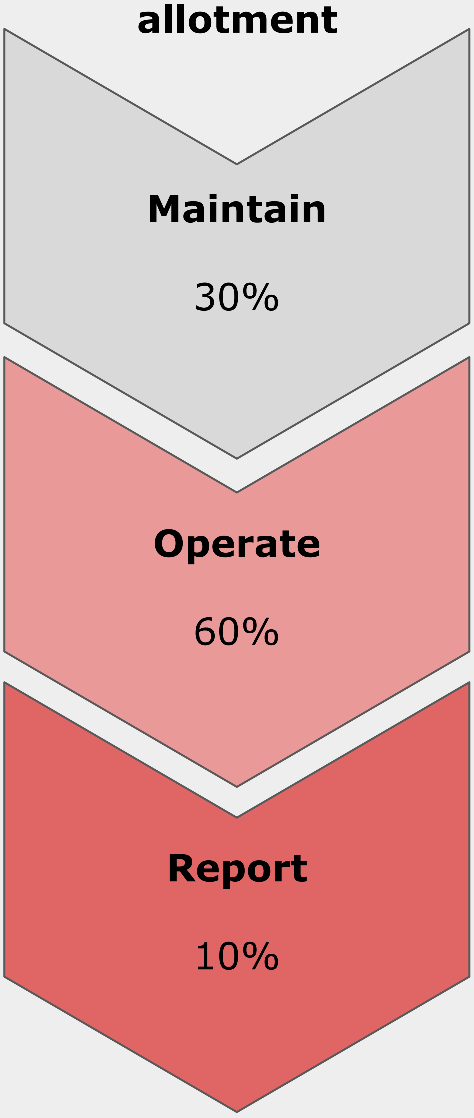
- Who do we need to report to?
- What are their reporting requirements?
- How much time is this taking us?

BlackHat Squirrel

https://github.com/blackhatsquirrel

It’s obviously impossible to say how much time should be assigned to each element of an operations department but guess what… we’ve only gone and done it anyway!

Ideal time to spend allotment



Maintain

30%

Operate

60%

Report

10%

If you’re spending more than 30% of your time maintaining your tools; either use them better or buy better tools.

The majority of your time should be spent here, the place where you can actually provide some value.

If more than 10% of your time is spent reporting you have 3 options:

1) Automate it
2) Convince management your time is better spent actually doing work
3) Quit

END OF DISCUSSION