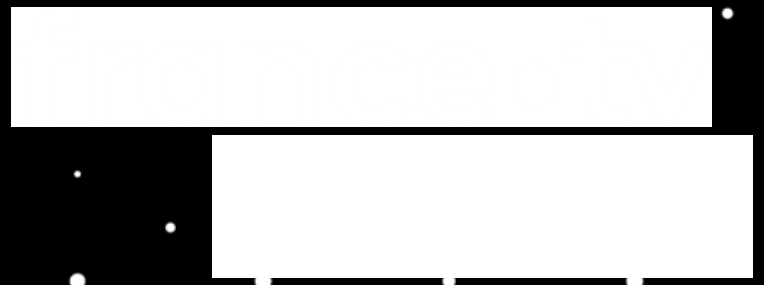


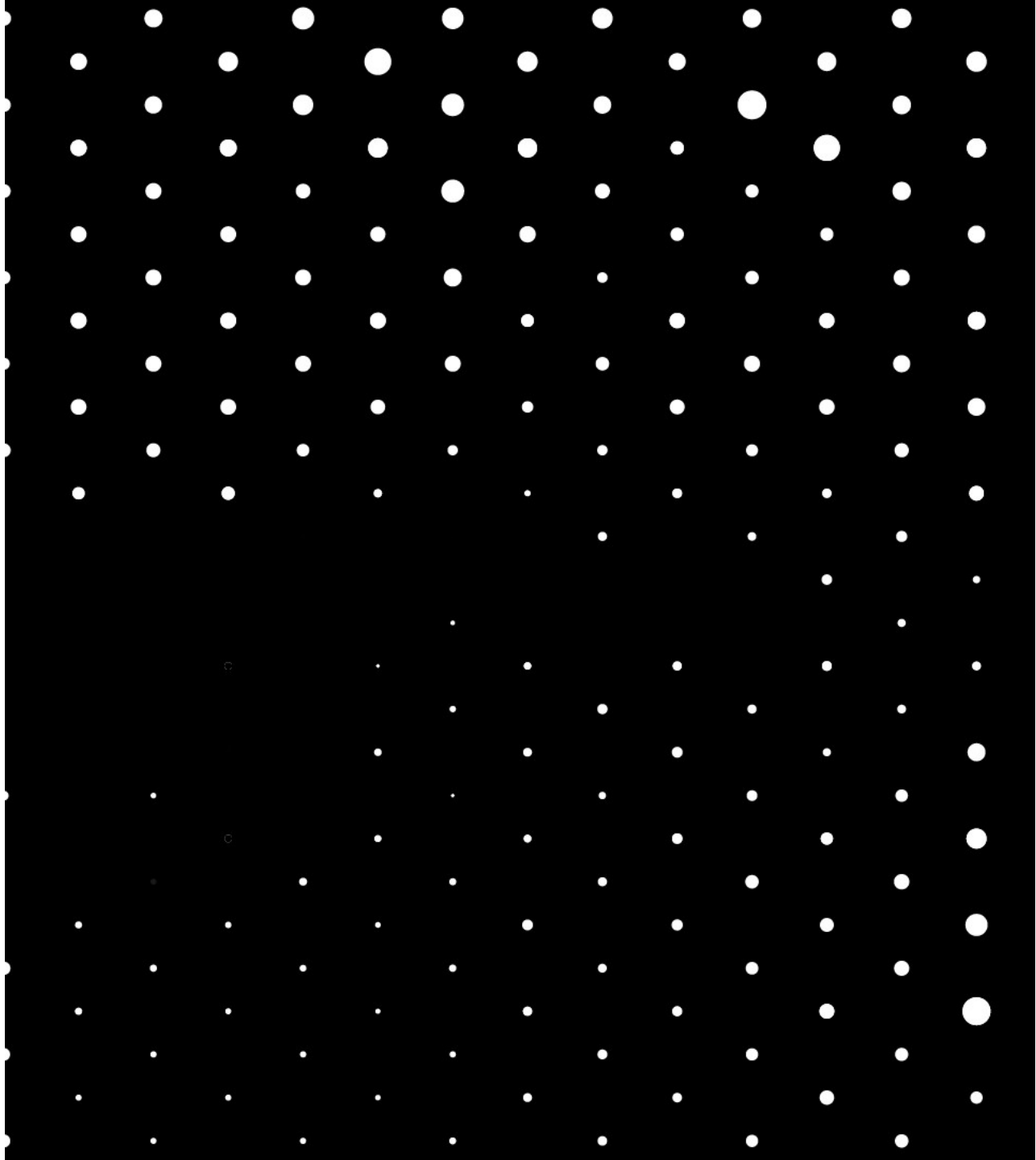
Two Years' Experience with a Media Company SOC

EBU MCS seminar 2019

Two years ago

01

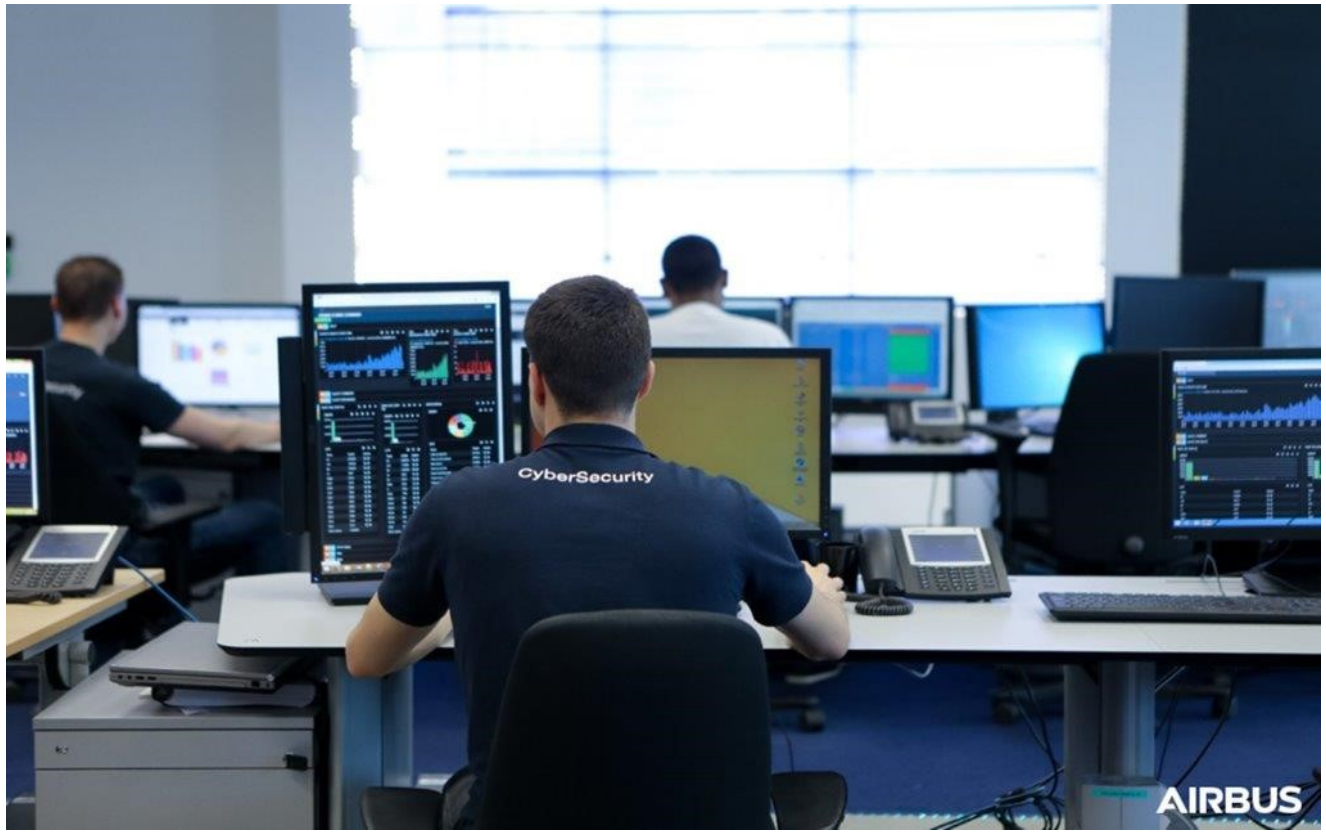
Why a SOC



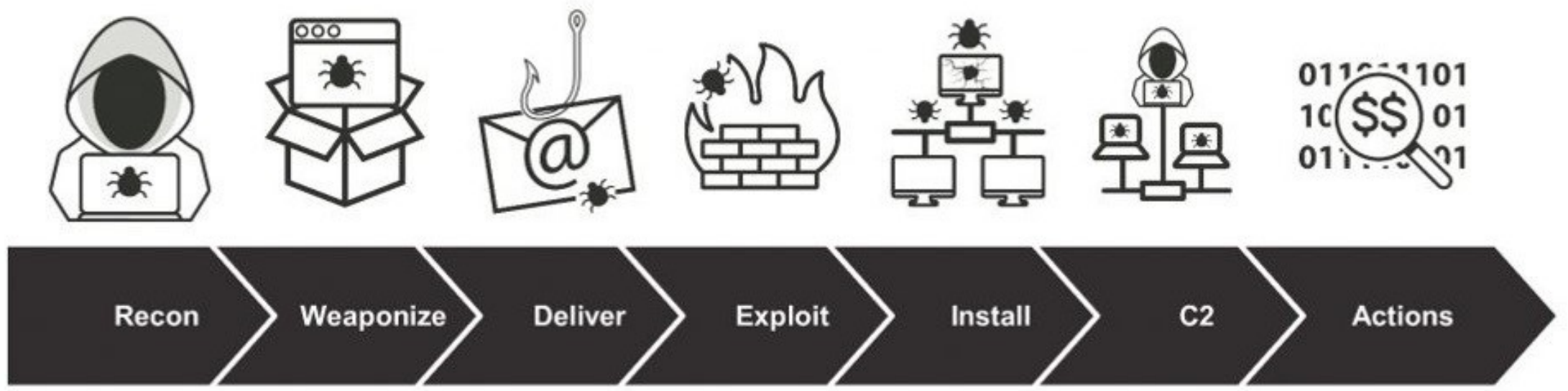
cybersec

It’s about incident response!!

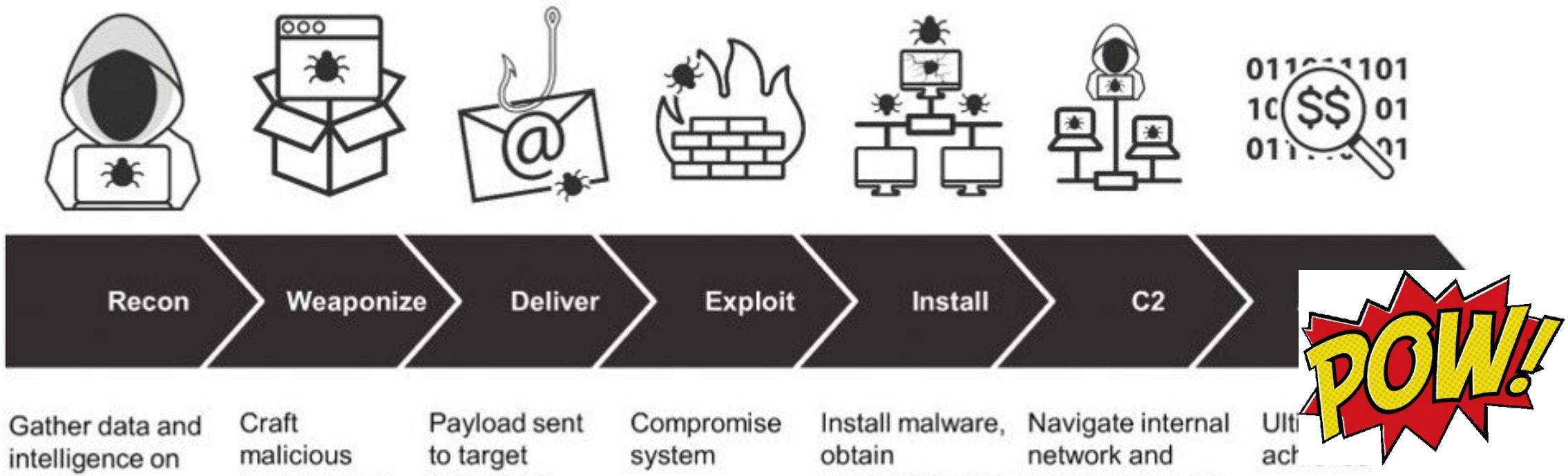
Security Operation Center



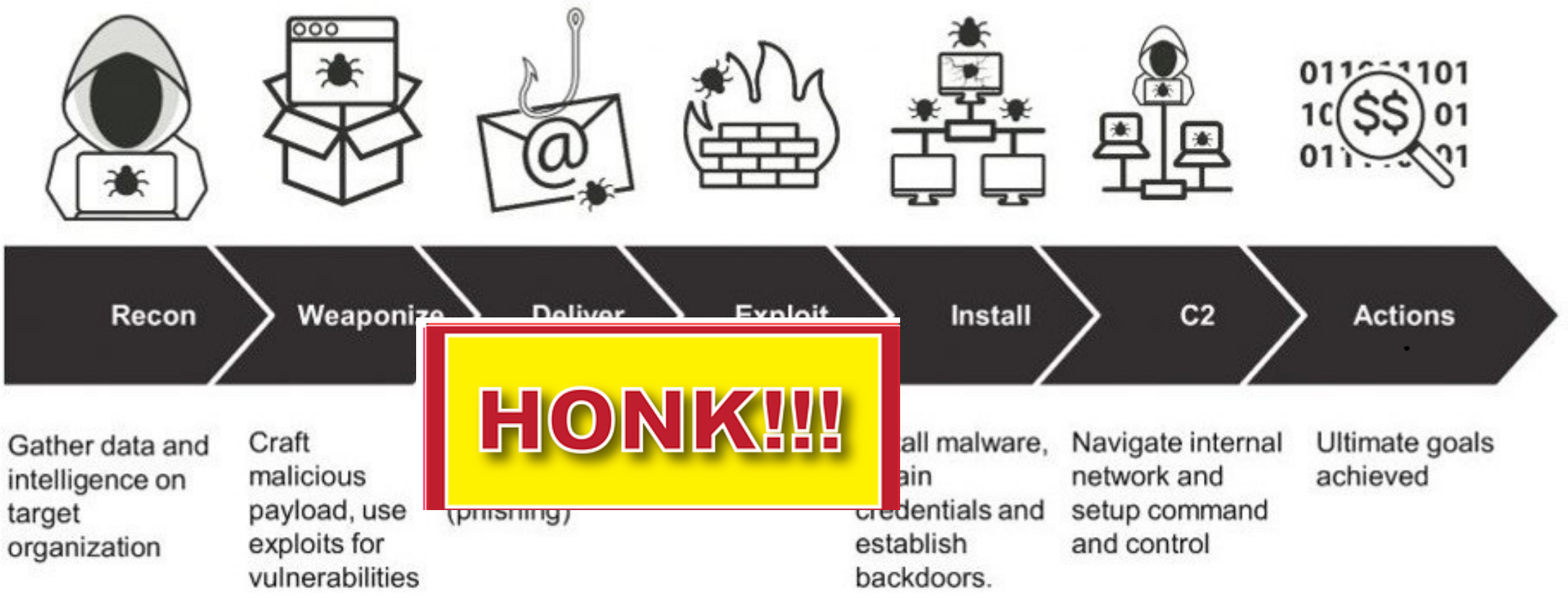
The kill chain



With no SOC

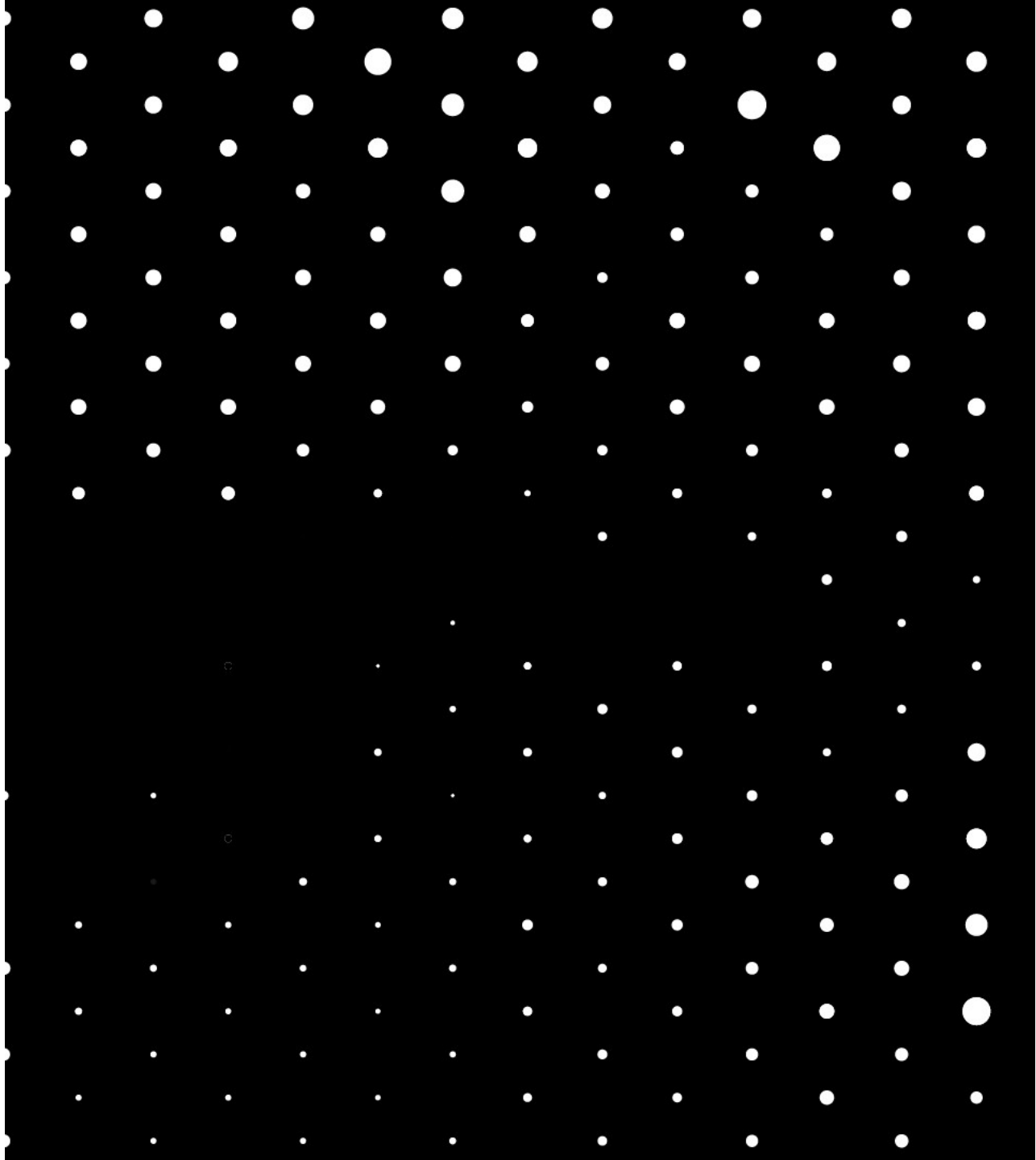

Recon
Weaponize
Deliver
Exploit
Install
C2
Gather data and intelligence on target organization
Craft malicious payload, use exploits for vulnerabilities
Payload sent to target (phishing)
Compromise system
Install malware, obtain credentials and establish backdoors.
Navigate internal network and setup command and control
POW!

With a SOC

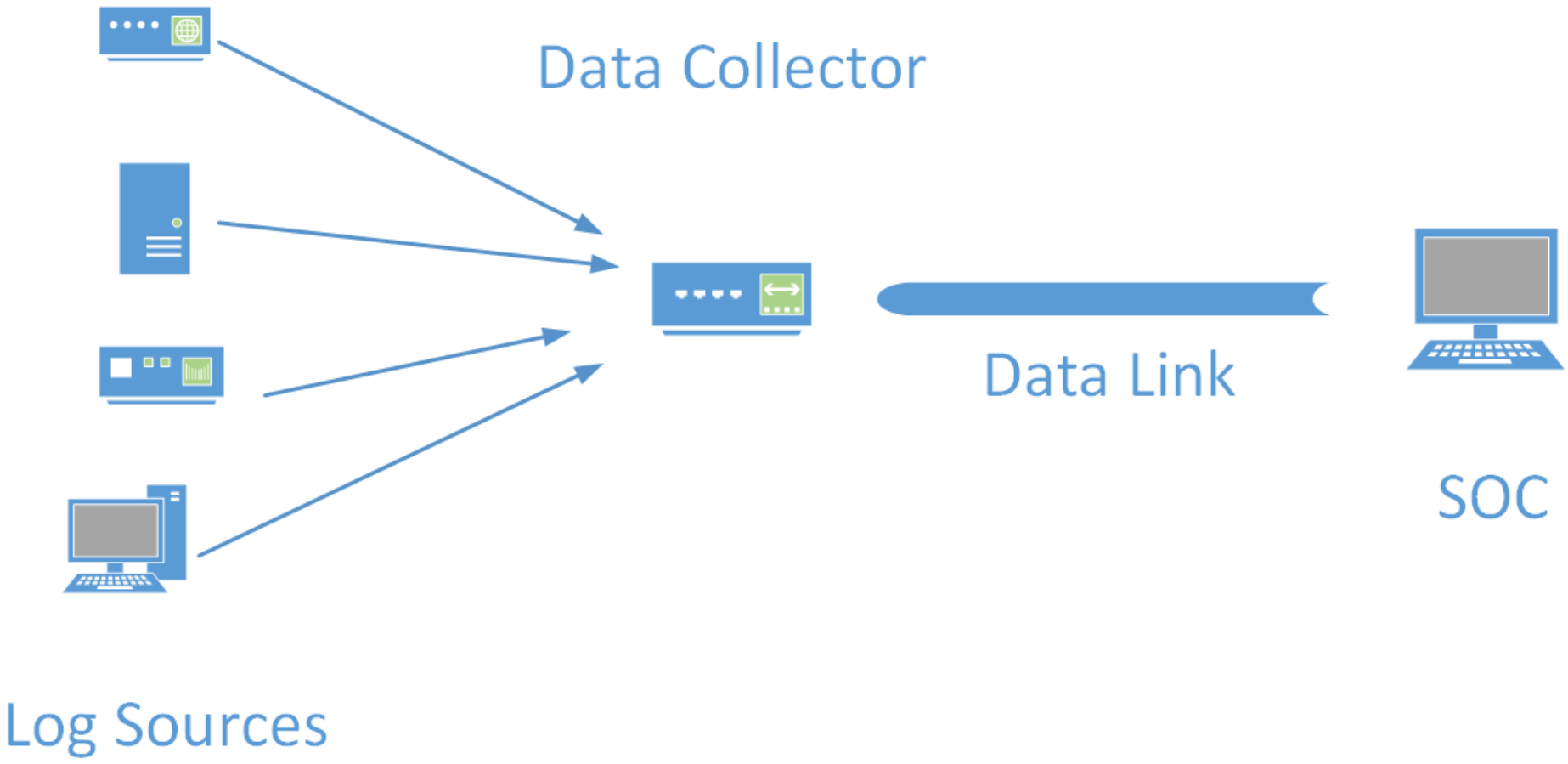

Recon
Weaponize
Deliver
Exploit
Install
C2
Actions
HONK!!!
Gather data and intelligence on target organization
Craft malicious payload, use exploits for vulnerabilities
(phishing)
all malware, ain credentials and establish backdoors.
Navigate internal network and setup command and control
Ultimate goals achieved

02

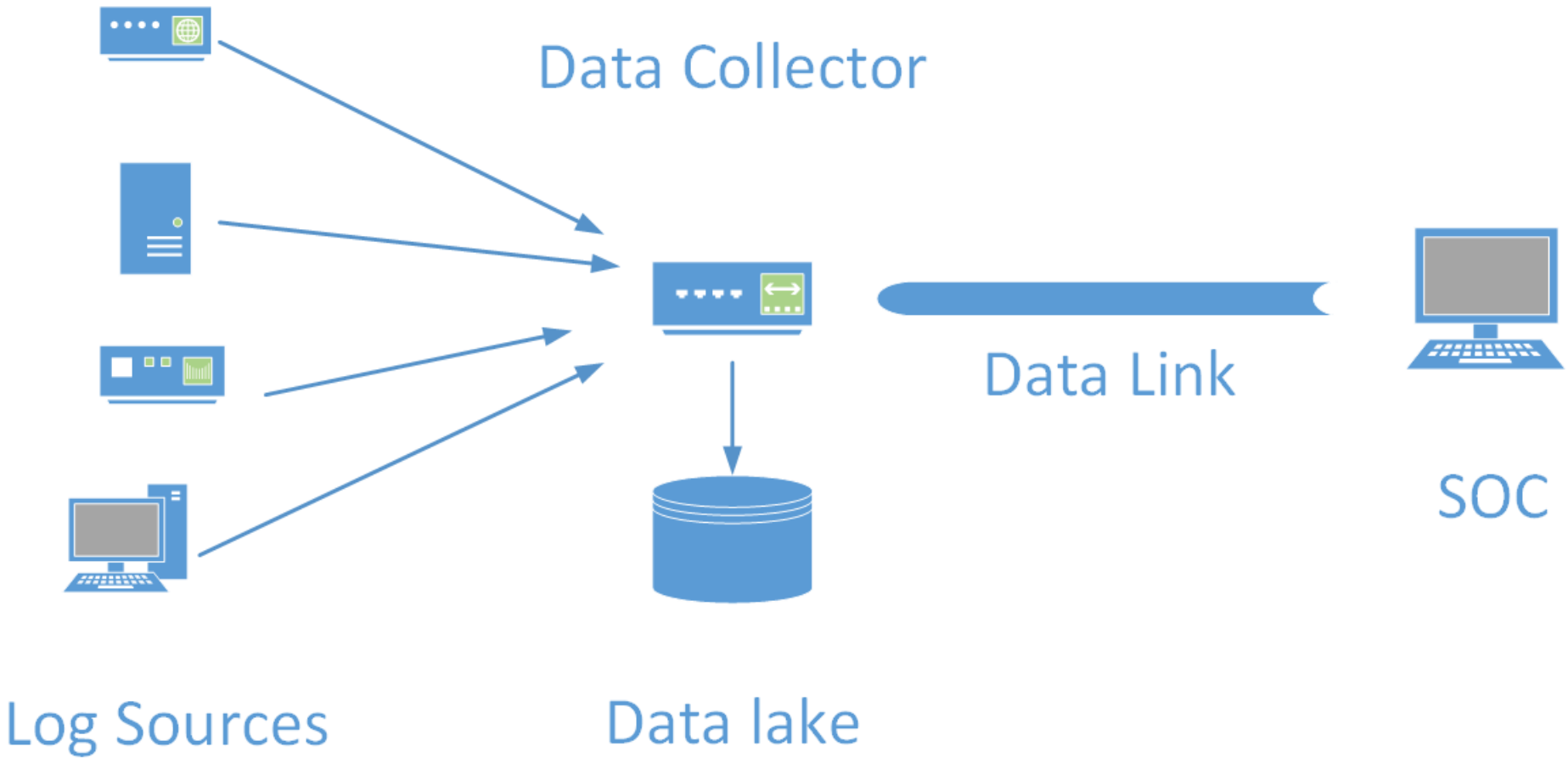
How does it work?



Collecting information

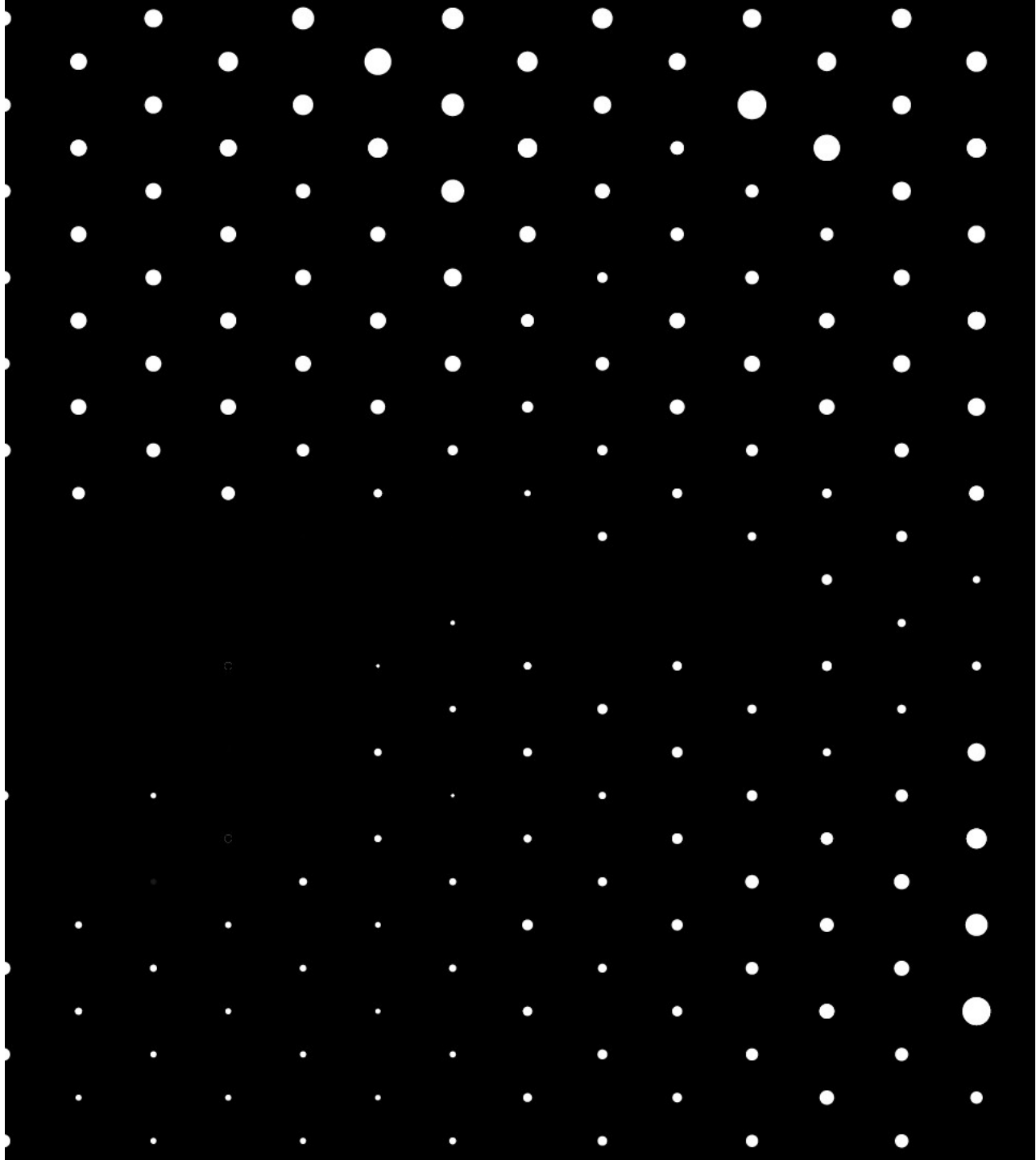


Collecting information



03

Building a SOC



cybersec

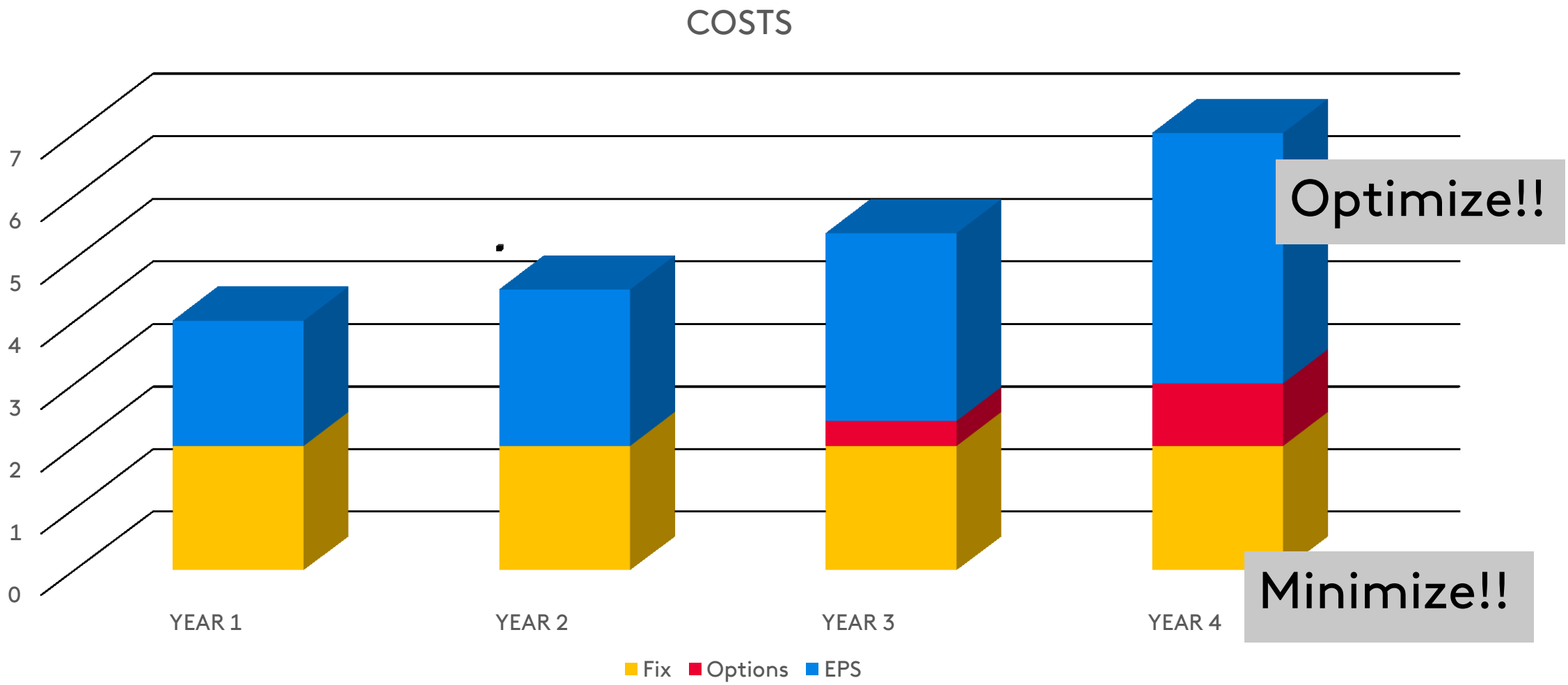
How much does it cost?

It costs a lot!!!

Compare with companies the same size than yours

Advice: Have a good, independant consultor with you!

Control the costs



Optimize with a risk based approach

More things to do

It'a a project!

- You need a project manager.
- You need a project team.

Collecting logs is not easy!

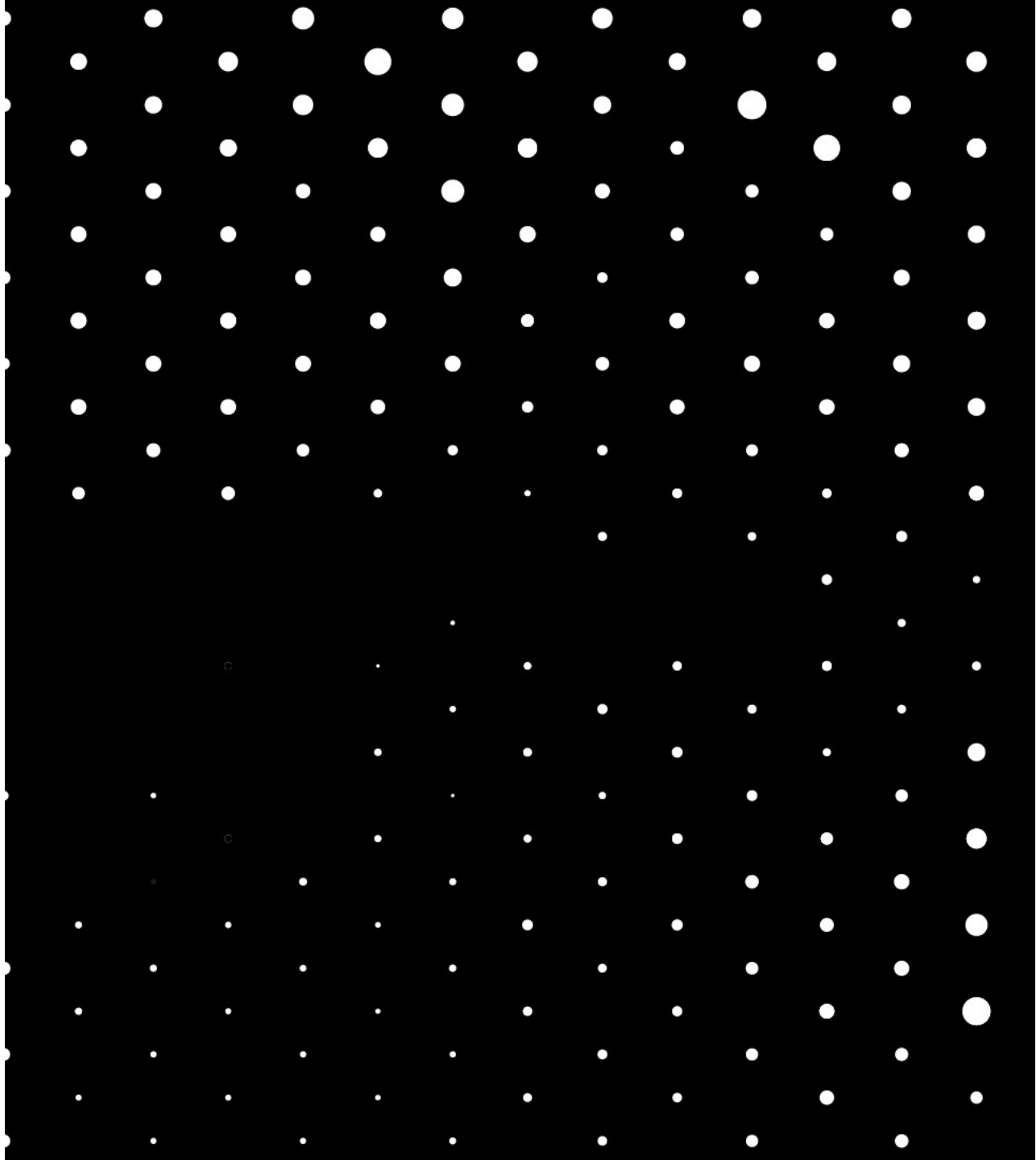
- You have to open ports...
- You have to configure OS
- The SOC must be able to parse

You need processes and procedures!

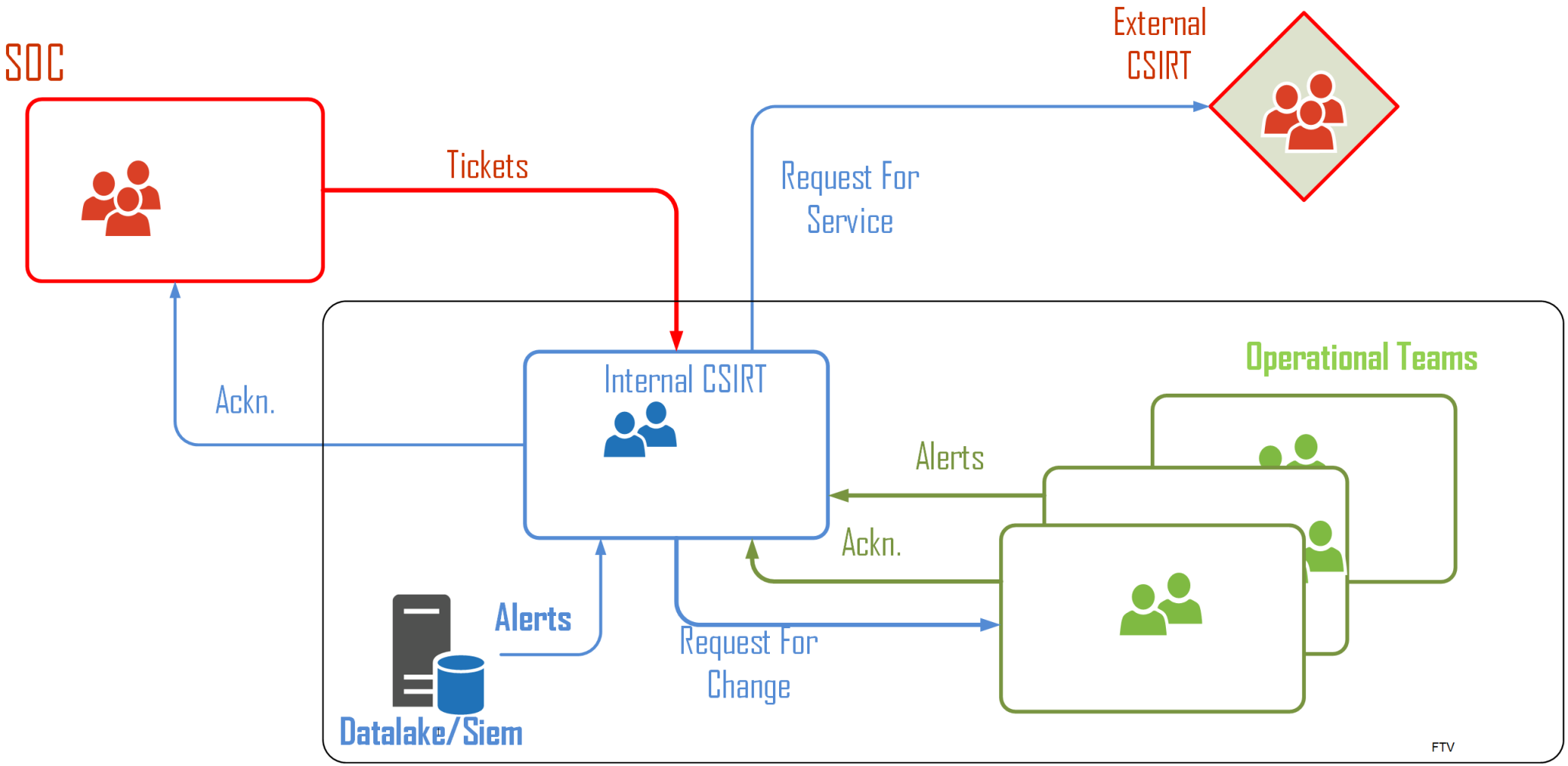
- Incident response
- Escalation

04

Running a SOC



You want your own response incident team!



Running a SOC

Its a continual improvement process!

Rules efficiency

New threats

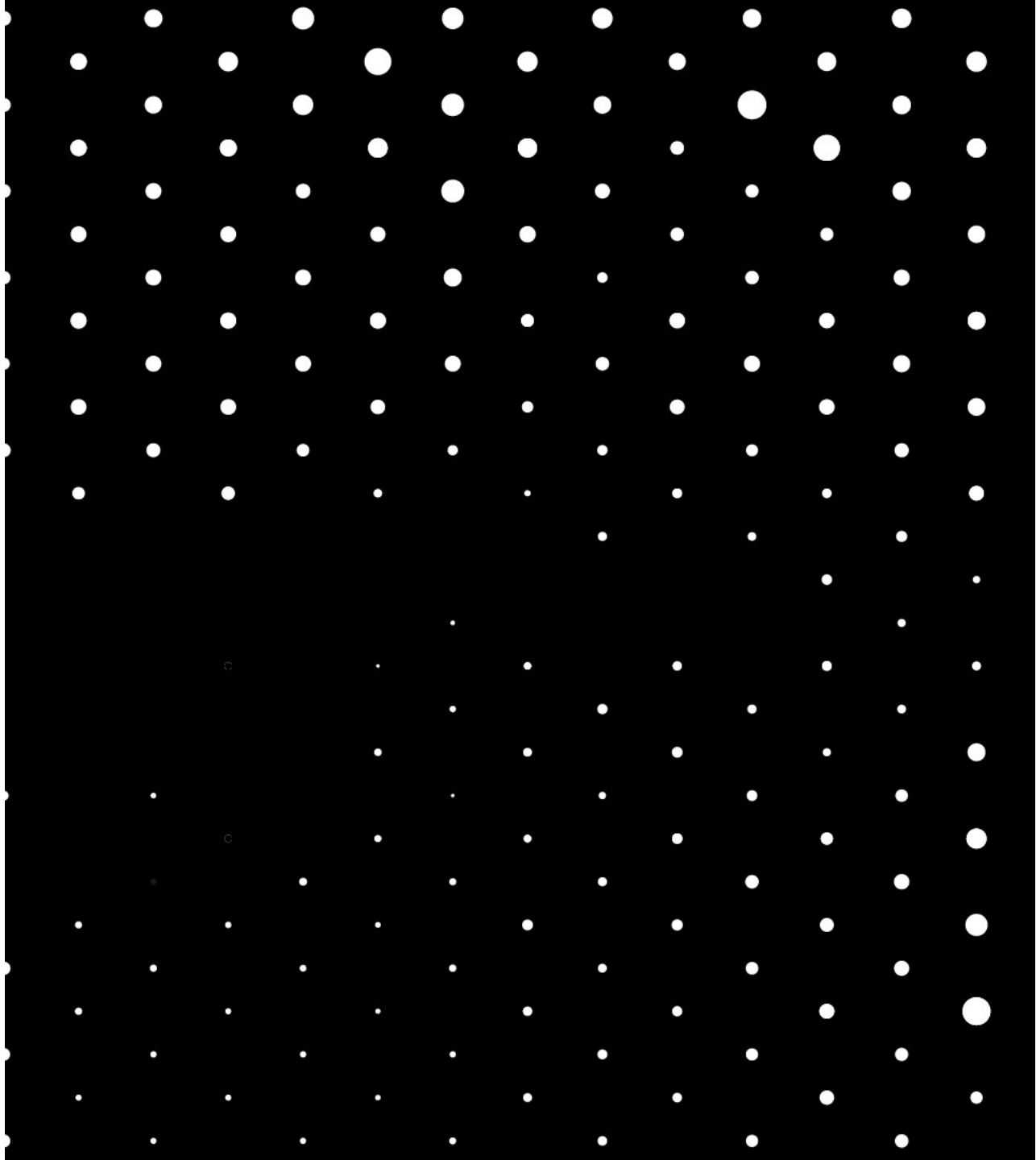
Pen tests

New Vulnerabilities

Infrastructure changes

05

Next Steps



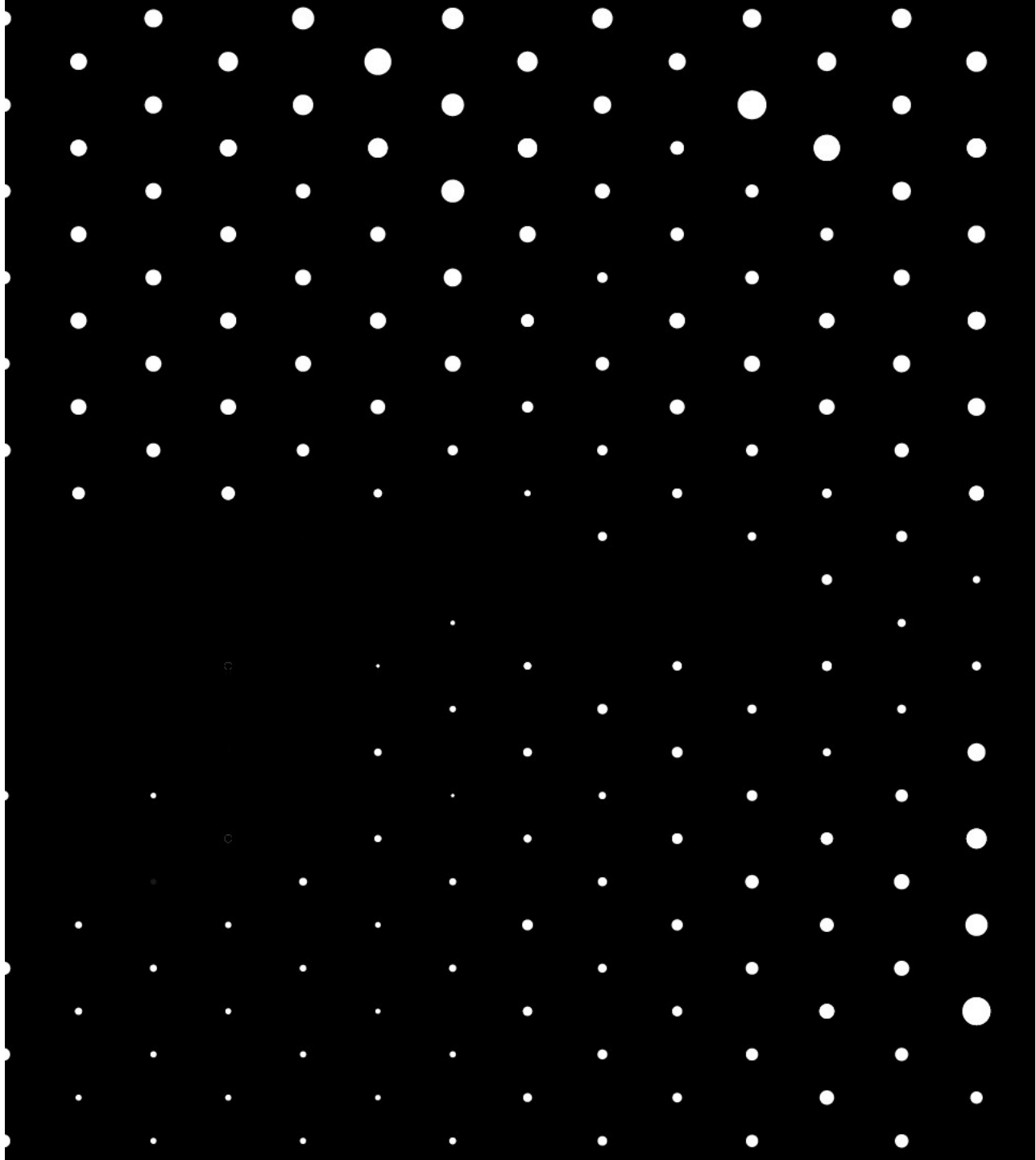
Next Challenges

Currently RFP for a new SOC

Is an external SOC the best solution?

06

Questions



cybersec