# DAVID THEJL-CLAYTON
# KEA TALK 2021-05-12


COMBITECH

# KEA TALK – 2021-05-12

## Chapter 1: Introductions

- Introduction to Me!
- Introduction to Combitech
- Introduction to the talk

## Chapter 2: 2nd Brain - CTI

- How to gather CTI?
- What is a 2nd Brain?
- Demo
- What can you do now?

## Chapter 3: Labbing

- Saga Lab
- Saga Lab – In Practice
- Saga Lab – Logging Experience
- Having your own lab

## Chapter 4: Applying for jobs

- CV advice
- Build a network
- Talk to people!

COMBITECH

# Chapter 1:

## Introductions

- Introduction to Me!
- Introduction to Combitech
- Introduction to the talk

# A LITTLE ABOUT ME…

British living in Denmark


Senior Advisor

Security Distractions…

Blogger

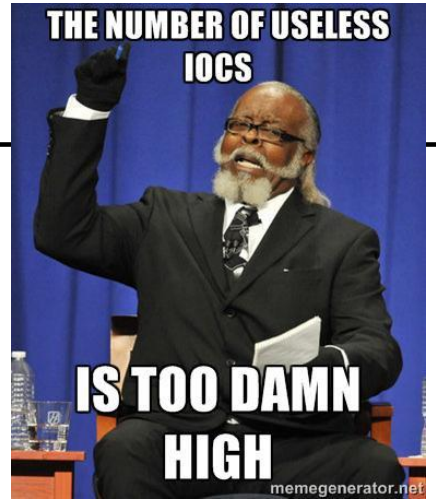
Open source


Teaching/Mentoring

# MY LIFE IN CTI/CYBERZ

2017

MISP Threat Sharing




2019

FOR578 CYBER THREAT INTELLIGENCE

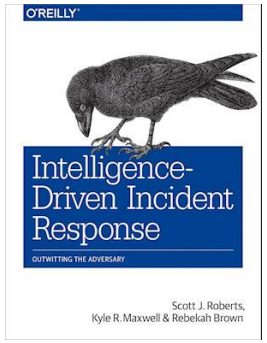
2020

Nordic Financial CERT

Threat Intelligence Committee

2020

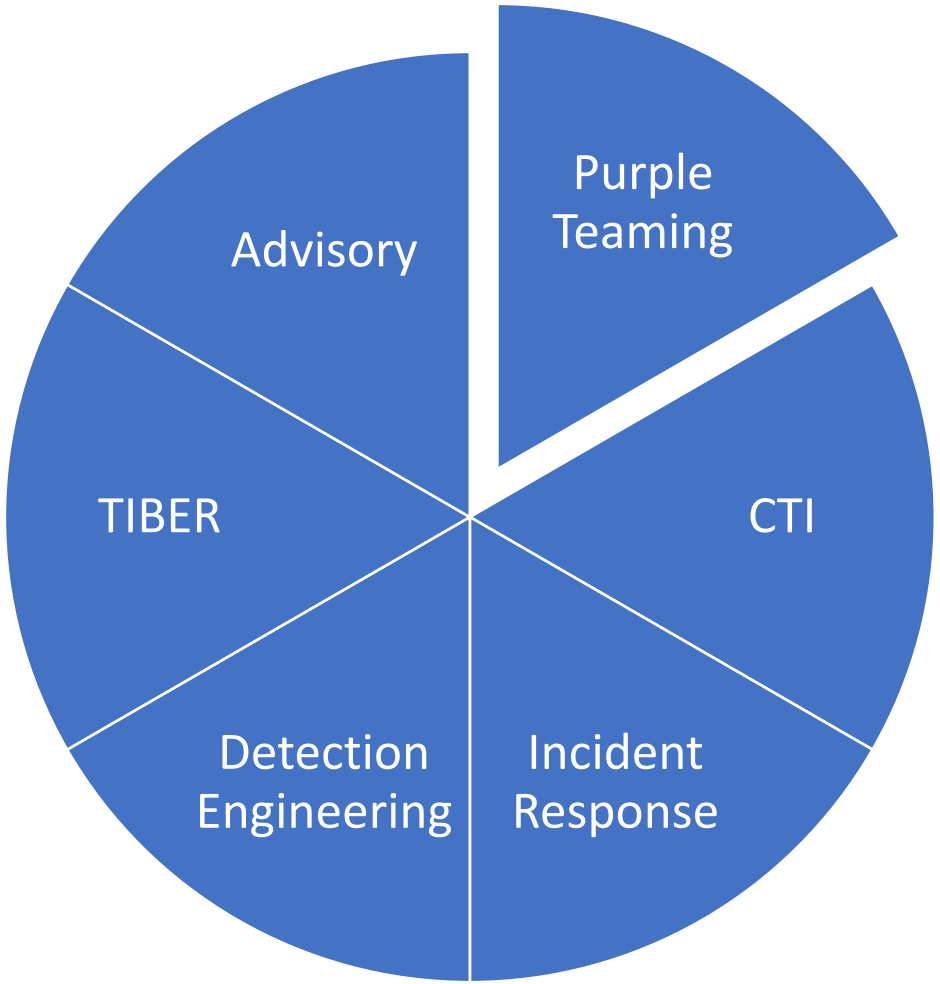
Intelligence Driven




2021

Moved to Combitech

# MY LIFE AT COMBITECH




# INTRODUCTION TO THIS TALK

I am tired…

…of giving talks where I am presenting expert material to students who might not get to work with it straight away…

Yes it might be exciting or inspiring, but I want to give you something you can use now!

# WHAT WILL TALK ABOUT THEN???

Today we will talk about ways that you as students can prepare for being set free into the Cyber Security world:-

- Gathering CTI for free…
  - 2nd brain technique (including demo)
  - How to do this yourself
- Labbing
  - Saga Lab
- Preparing for job applications
  - CV Advice
  - Building a network

# Chapter 2:

## 2nd Brain - CTI

- How to gather CTI?
- What is a 2nd Brain?
- Demo
- What can you do now?

# WHAT IS CTI (CYBER THREAT INTELLIGENCE?)

When we talk about Threat Intelligence, it is important to remember what Threat Intelligence actually is!

**Threat Data**

Indicators (IP, Domain, etc)

- Data about threats others have seen but without context.

How can we use this? Why is it important to us?

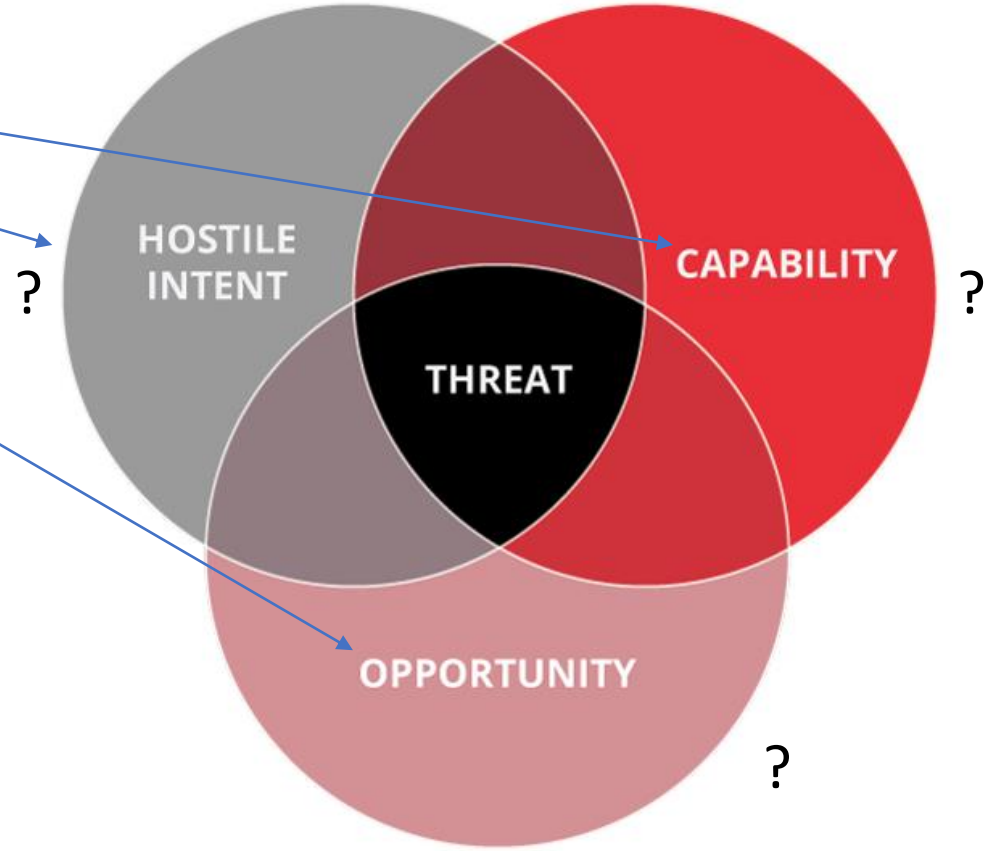
- A long list of IP's which are on a block list, is it useful to us?

# WHAT IS THREAT DATA

**101.24.100.101**

Is this something we should act on?

There is something missing before we can take a decision on how to treat this data….



# THREAT INTELLIGENCE

For Threat Intelligence to be valuable it must:

- Have context
- Be relevant

To achieve this you need to take threat data and apply the context:

- This IP address has been seen hosting a ransomware payload and this actor is known to target our sector.

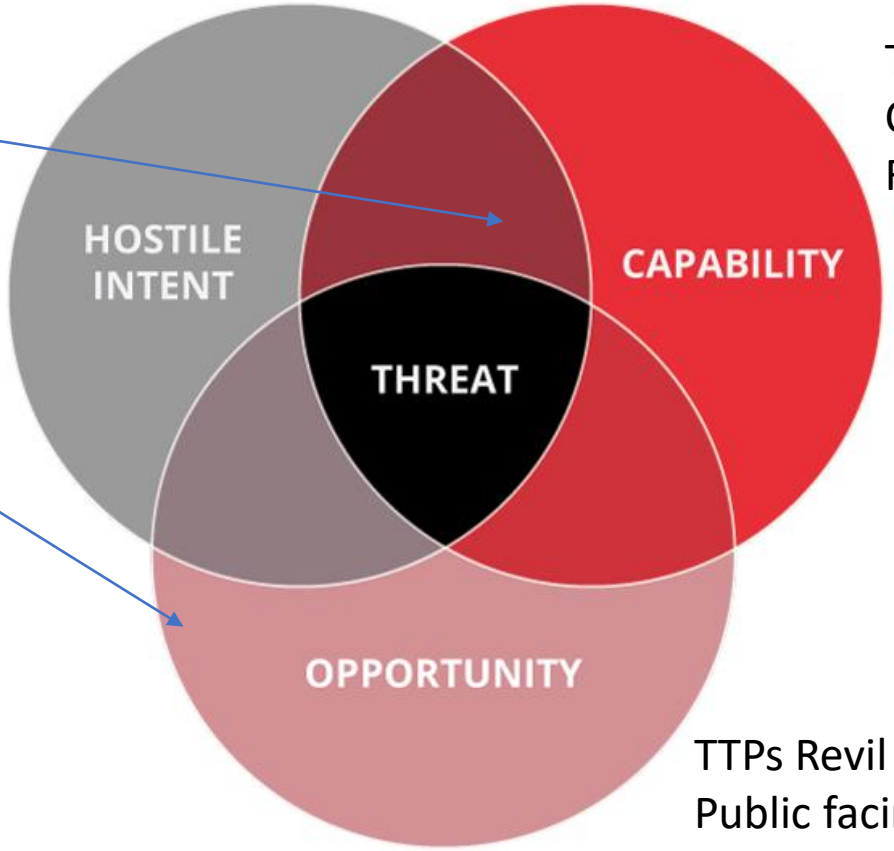
# WHAT IS THREAT INTELLIGENCE

**101.24.100.101**

Is this something we should act on?

Yes, we know that REvil is targetting our sector

Ransomware

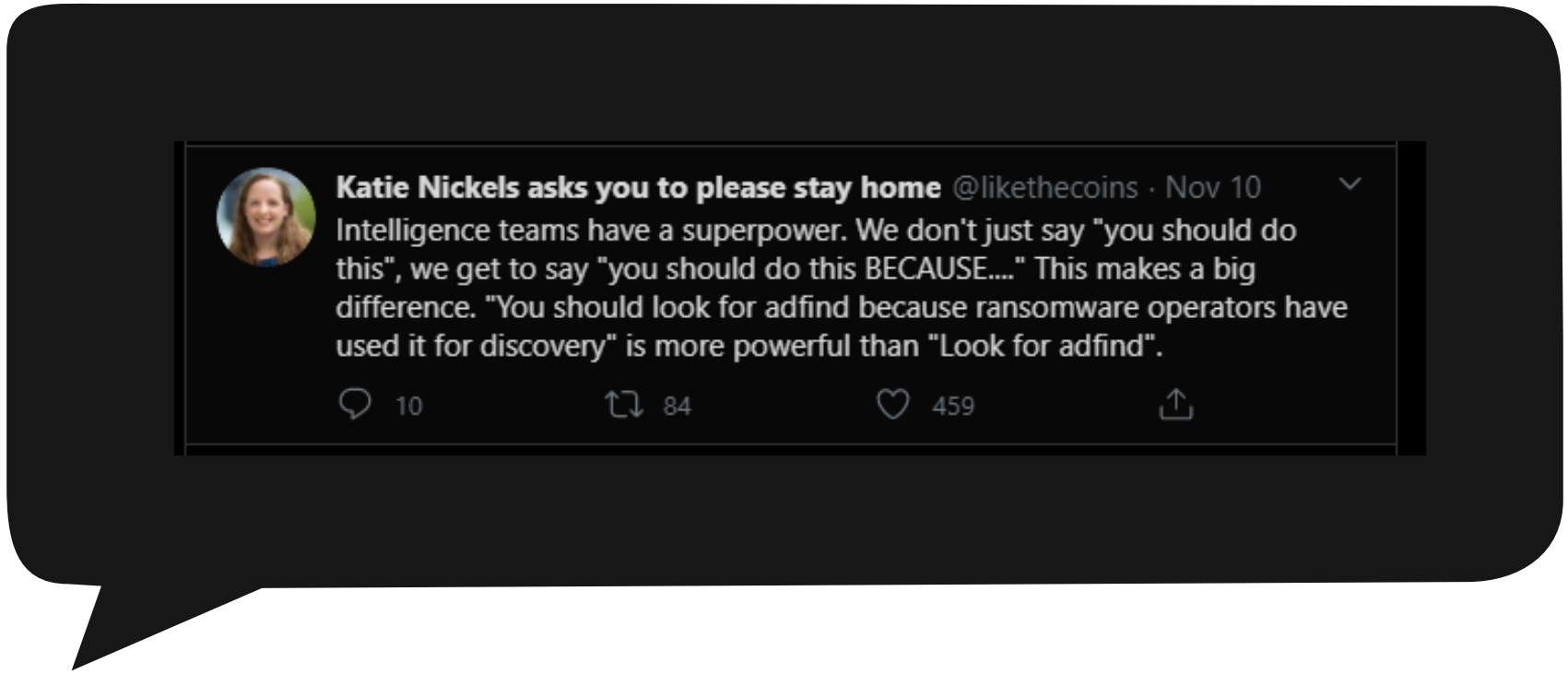



TTPs Revil
C2
Framework

TTPs Revil
Public facing vuln



COMBITECH


Katie Nickels asks you to please stay home @likethecoins · Nov 10
Intelligence teams have a superpower. We don't just say "you should do this", we get to say "you should do this BECAUSE...." This makes a big difference. "You should look for adfind because ransomware operators have used it for discovery" is more powerful than "Look for adfind".
10
84
459

# HOW TO GATHER CTI?

The best place to gather CTI is from your own incidents…

However you don’t have this…

The next best place to gather CTI is from your network…

However you don’t have this…

But there is another way to do it…

# HOW TO GATHER CTI?

- Read everything that you can...
  - News
  - Blogs
  - Twitter
  - Reports
- Decide on what you want to focus on, bring your own context…
  - Ransomware gangs?
  - Malware variants?
  - Sector specific attacks?

# WHAT THEN?

Reading articles is great, but how can you remember it all?

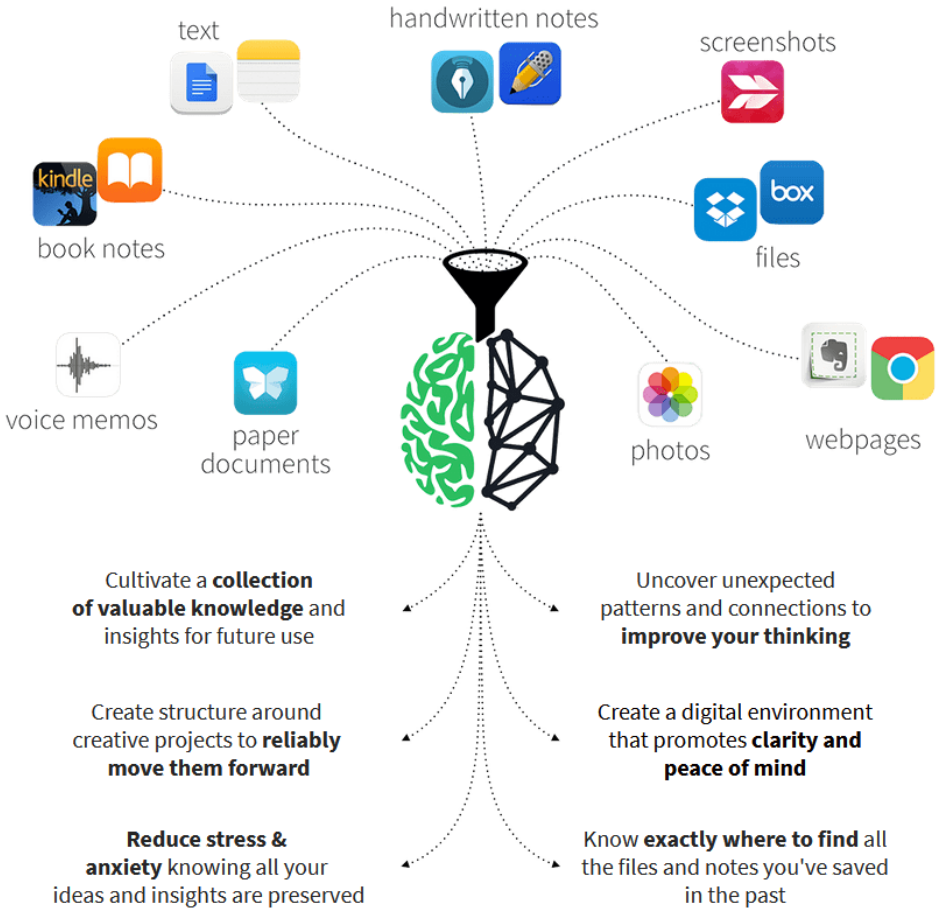
How can you make your knowledge more operational and useful?

You are going to need a 2nd brain!

# 2ND BRAIN

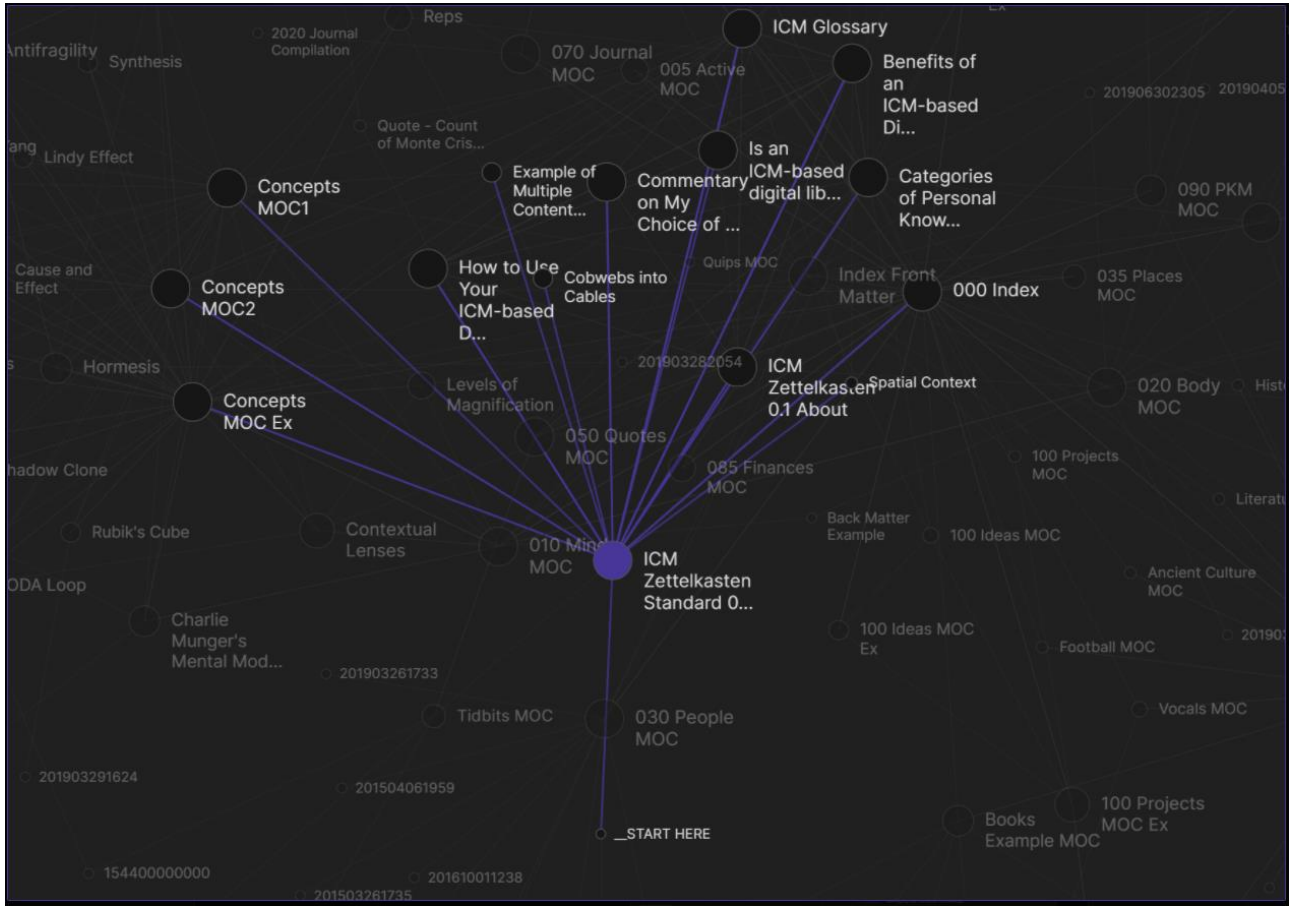
The idea is that we consume so much information everyday that we simply cannot remember it all...

So why not spend a few extra minutes indexing it!




Source: http://chuckfrey.com/how-building-second-brain-blew-thinking/

# OBSIDIAN - DEMO



# WHAT CAN YOU DO NOW?

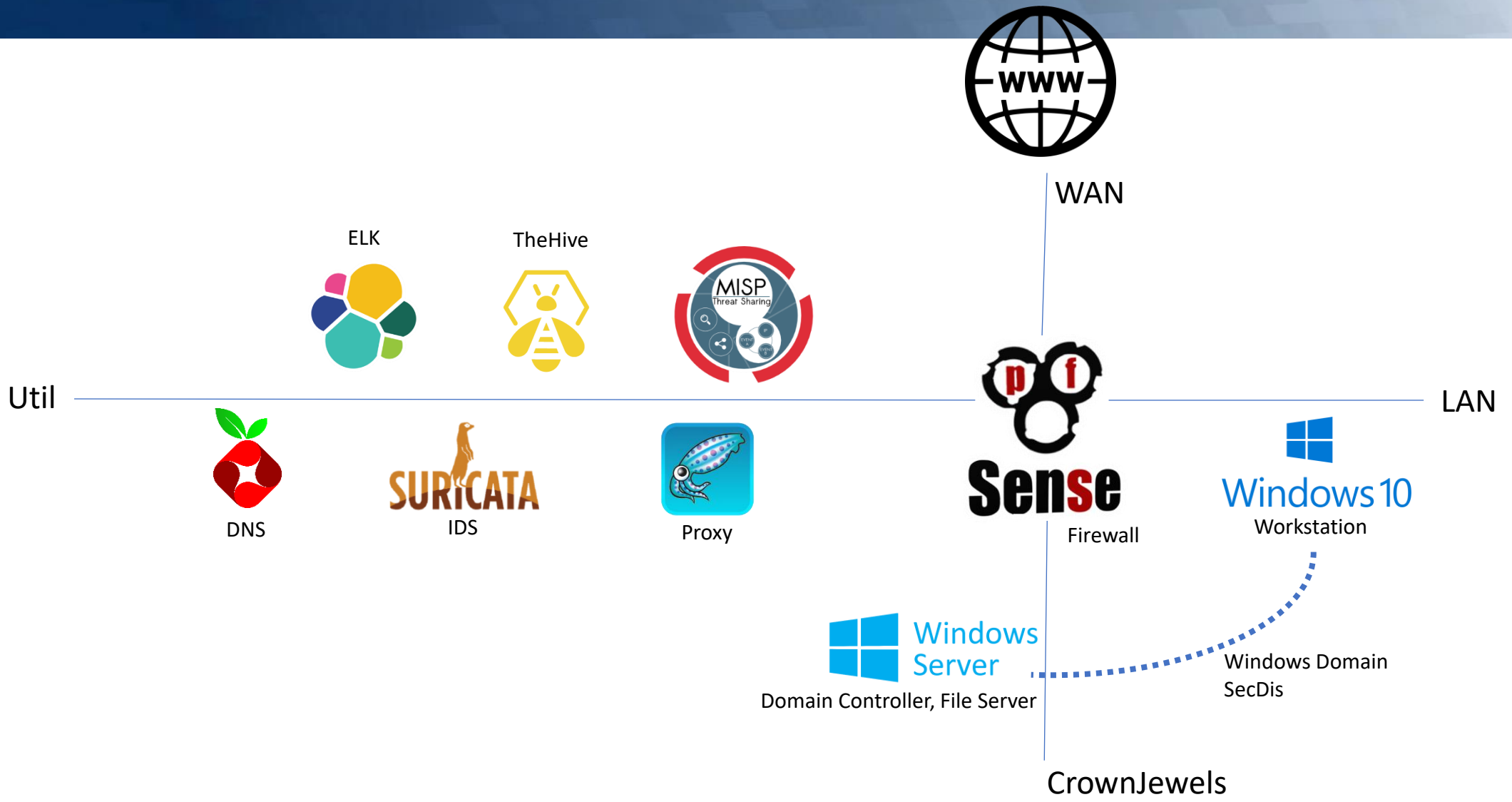
- Download Obsidian!
- Find your context
- Find your resources (Blogs etc)
- Get indexing!

# Chapter 3

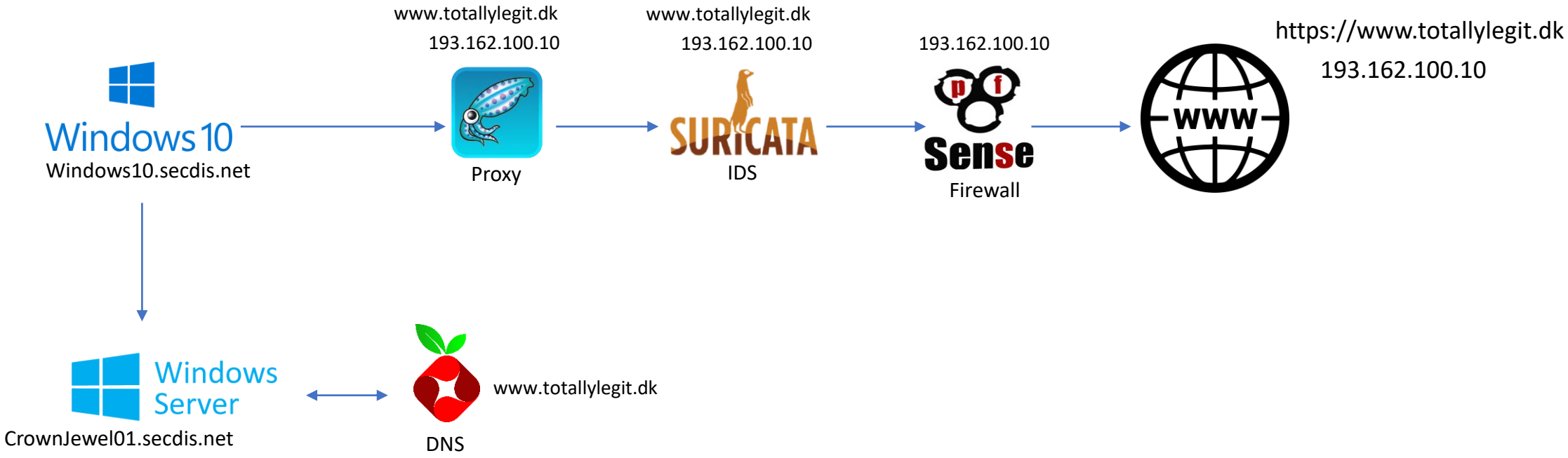
## Having your own Lab

- Saga Lab
- Saga Lab – In practice
- Saga Lab – Logging experience
- Having your own lab

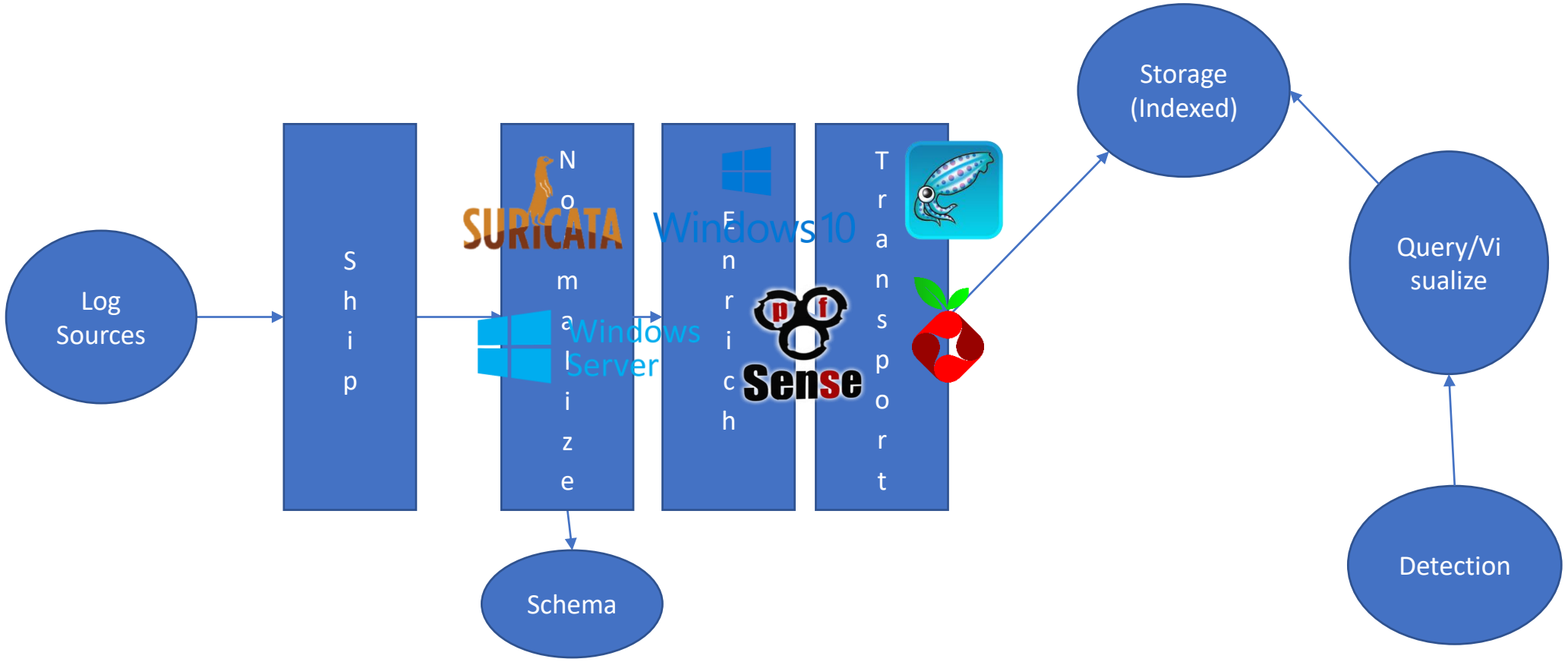
# SAGA LAB


WAN
ELK
TheHive
MISP
Threat Sharing
Util
LAN
DNS
IDS
SURICATA
Proxy
Sense
Firewall
Windows 10
Workstation
Windows
Server
Domain Controller, File Server
Windows Domain
SecDis
CrownJewels

# SAGA LAB – IN PRACTICE



# SAGA LAB – LOGGING EXPERIENCE



# HAVING YOUR OWN LAB

What do you get out of building your own lab?

- Hands on experience with tools
- Ability to test malware (be safe) and see what happens
- Fill your time whilst applying for jobs

# Chapter 4

## Applying for jobs

- CV advice
- Build a network
- Talk to people!

# CV ADVICE

- Keep it to the point!
  - You do not have so much experience to write about…
  - Bullet points are king!
- Mention the things you do outside of your studies
  - Lab?
  - Open source work?
  - CTI knowledge?
  - Blogging?

# BUILD A NETWORK

In Denmark, most jobs are filled by networking…

- Join up to the VSEC Discord
- Attend OWASP meetings
  - Copenhagen
  - Aarhus
- Join the “New Born Cybersec Professionals” network on LinkedIn
- If you don’t have a LinkedIn profile, get one…
  - Denmark is mad for LinkedIn

# TALK TO PEOPLE!

- When you have built your network, use it!

- Reach out to people for advice
  - VSEC Discord
  - LinkedIn
- Arrange virtual coffees to discuss topics
- Ask for advice!

# DAVID'S CAREER WORKSHOP

If there is a desire/demand, I will happily setup a career workshop where we can discuss this further!

# COMBITECH


COMBITECH.DK | .SE | .FI | .COM