

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!

Chapter 1:

Introductions

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

COMBITECH

A LITTLE ABOUT ME...



British living in Denmark



Senior Advisor

Security
Distractions...

Blogger



Open source

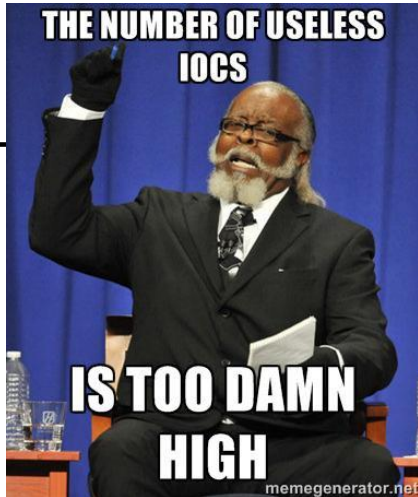


Teaching/Mentoring

MY LIFE IN CTI/CYBERZ



2017



2019

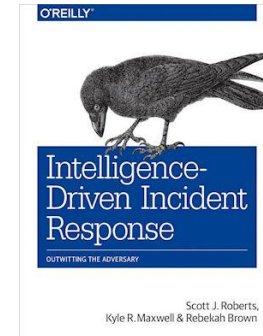


2020

Threat
Intelligence
Committee

Intelligence
Driven

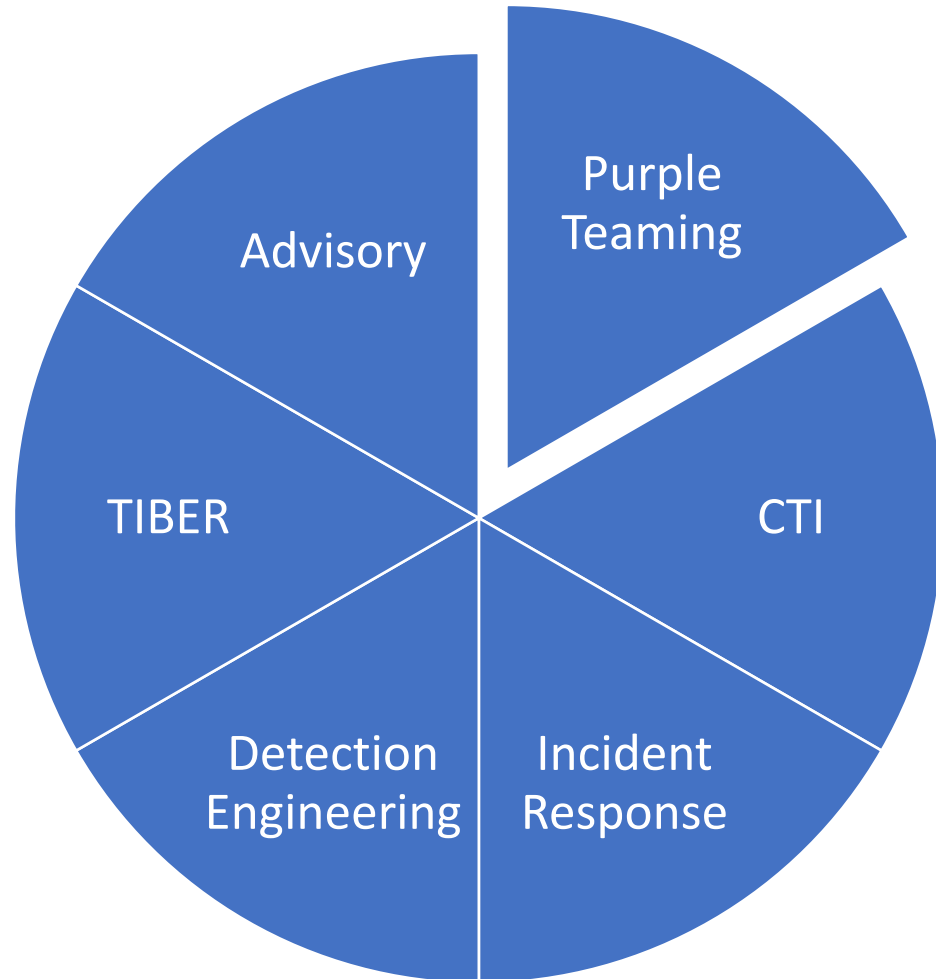
2020



2021

Moved to
Combitech

MY LIFE AT COMBITECH



COMBITECH

COMBITECH

OM COMBITECH



Nordisk leder indenfor IT-sikkerhed

Combitech er med sine 2000 medarbejdere, heraf 300 dedikerede IT-sikkerhedsspecialister, Nordens største uvildige konsulentvirksomhed på IT-sikkerhedsområdet og leverer uvildig rådgivning med dyb sektorviden og sektorspecifikke services.

Vi har gennem de seneste 30 år udøvet betroet rådgivning med et primært fokus på den finansielle sektor, energisektoren, central offentlig forvaltning, globale produktionsvirksomheder samt forsvarsindustrien.

Sikkerhed er i vores DNA

Combitech er en uvildig og uafhængig del af Forsvars- og Sikkerhedsindustrien Saab AB og vores forankring i forsvarsindustrien betyder, at vi har unikke kompetencer indenfor bl.a. Threat Intelligence sikring af kritisk infrastruktur.

Vi har stor erfaring med udarbejdelse af komplekse IT-sikkerhedsprogrammer og rådgivning indenfor sektorfokuserede og -specialiserede IT-sikkerhedsområder hvor specifikke krav skal implementeres ud fra best-practise guidelines og regulatoriske krav for den enkelte sektor.

Sikkerhed med et formål

Vores mål er at etablere partnerskaber med vores kunder og hjælpe med at sikre et risikobaseret og modstandsdygtigt IT-sikkerheds set-up på tværs af virksomheden. Vi har ansat dedikerede sektoreksperter med mange års erfaring på topledelsesniveau for at sikre, at vi kan binde IT-sikkerhed og forretnings sammen.

Best in Class kompetencer

Vi vil være bedst – og vi tilbyder en høj leverancekapacitet, en bred palette af specialistkompetencer og best-in-class leverancekvalitet.

Alle Combitechs medarbejdere bliver ved ansættelsen sikkerhedsgodkendt af Forsvarets Efterretningstjeneste (FE) samt af Saab Group interne sikkerhedsafdeling.

Vi er certificerede inden for ISO 27001, ISO 9001 samt ISO17025 og vores medarbejdere har certificeringer indenfor: CISM, CRISC, CISA, CIPT, CIPM, CIPP/E, CISSP, CCSP, OSCP, OSCE



A TRUSTED PARTNER

Combitech er en betroet samarbejdspartner for virksomheder af alle størrelser på tværs af flere sektorer



CYBER SECURITY AS-A-SERVICE

Combitech tilbyder IT-sikkerhed som en service – en moderne, kontrolleret og nem måde at sikre virksomheder på



NORDIC CYBER SECURITY LEADER

Med mere end 300 konsulenter er Combitech Nordens største leverandør af uvildig rådgivning på IT-sikkerhedsområdet



COMBITECH

COMBITECH

IT-SIKKERHED SERVICES

- Ledelsesrådgivning: Strategi, It-sikkerhedspolitik, it-risikostyringspolitik og it-sikkerhedshåndbog
- Trusselsanalyse og Risikovurderinger
- Ledelsesrapportering for efterlevelse af lovgivning og compliance-tjek
- Katastrofe- og beredskabsplan
- Bestyrelsesworkshops
- CISO as a Service

Industri-specifik
ledelsesrådgivning

Identificering af
potentielle trusler
og sårbarheder

- Risiko & modenhedsanalyse
- Simulerede Threat Intelligence baseret cyber angreb, Red Team
- Teknisk Health Check fx AD, Privilegerede brugere
- Compliance Audit og 3rd party risk
- Simulerede Phishing angreb
- Tekniske Pentests

- Cyber Strategi, politik, processer og procedurer
- Secure Development Lifecycle
- Privilegeret brugeradgang
- SOC design/implementering
- IT / OT teknisk security design / implementing
- Cyber og informationssikkerheds awareness / træning

Styrke organisationens
cyber robusthed

Detektering og
respondering ved
cyber angreb

- Sårbarhedsanalyse
- Threat Intelligence Services
- Overvågning af it-sikkerhedshændelser /Managed Detection & Response Services
- Incident Response & Forensics Services

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?

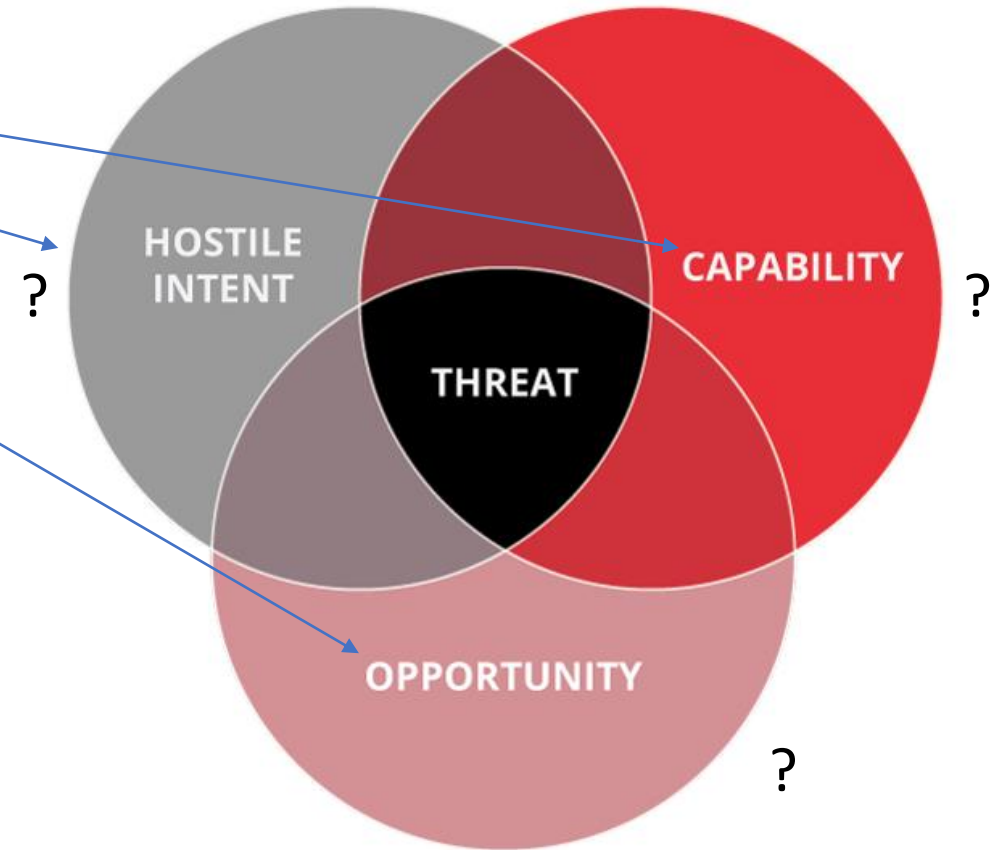
- A long list of IP's which are on a block list, is it useful to us?

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.

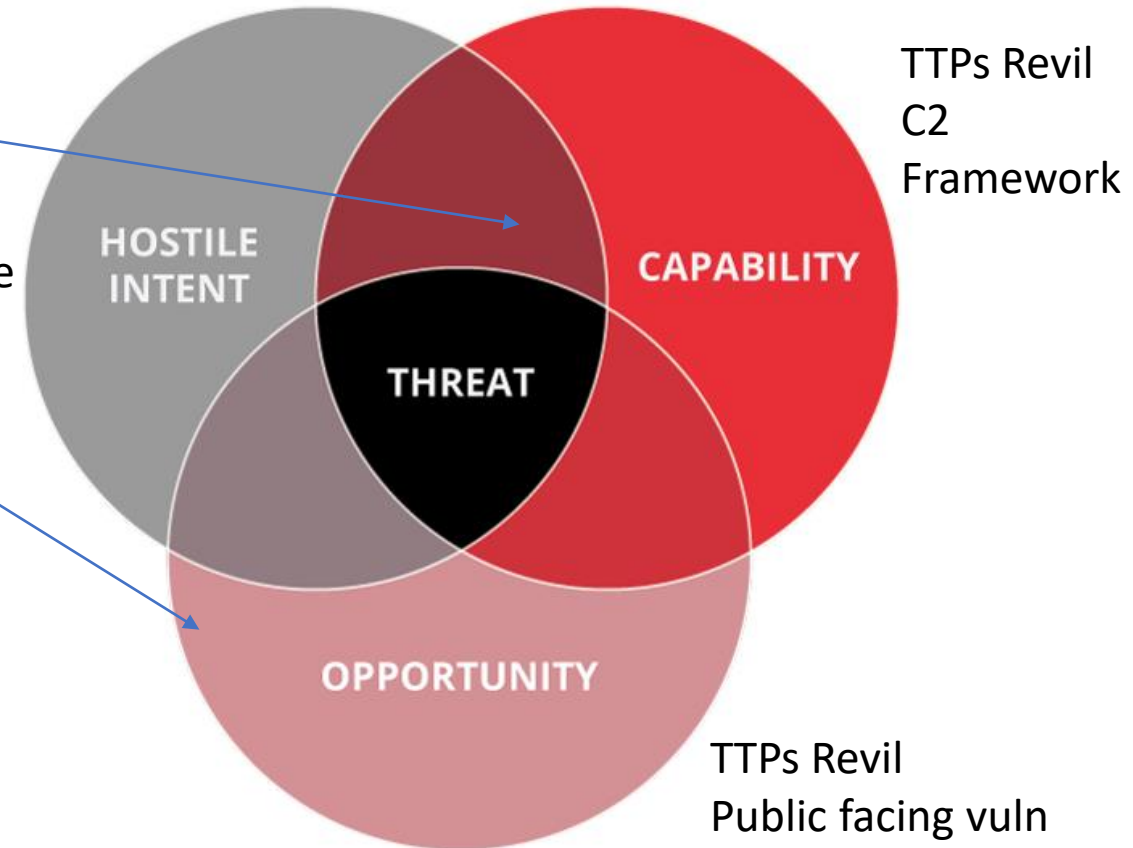
WHAT IS THREAT INTELLIGENCE

101.24.100.101

Is this something we should act on?

Ransomware

Yes, we know that REvil is targetting our sector





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?

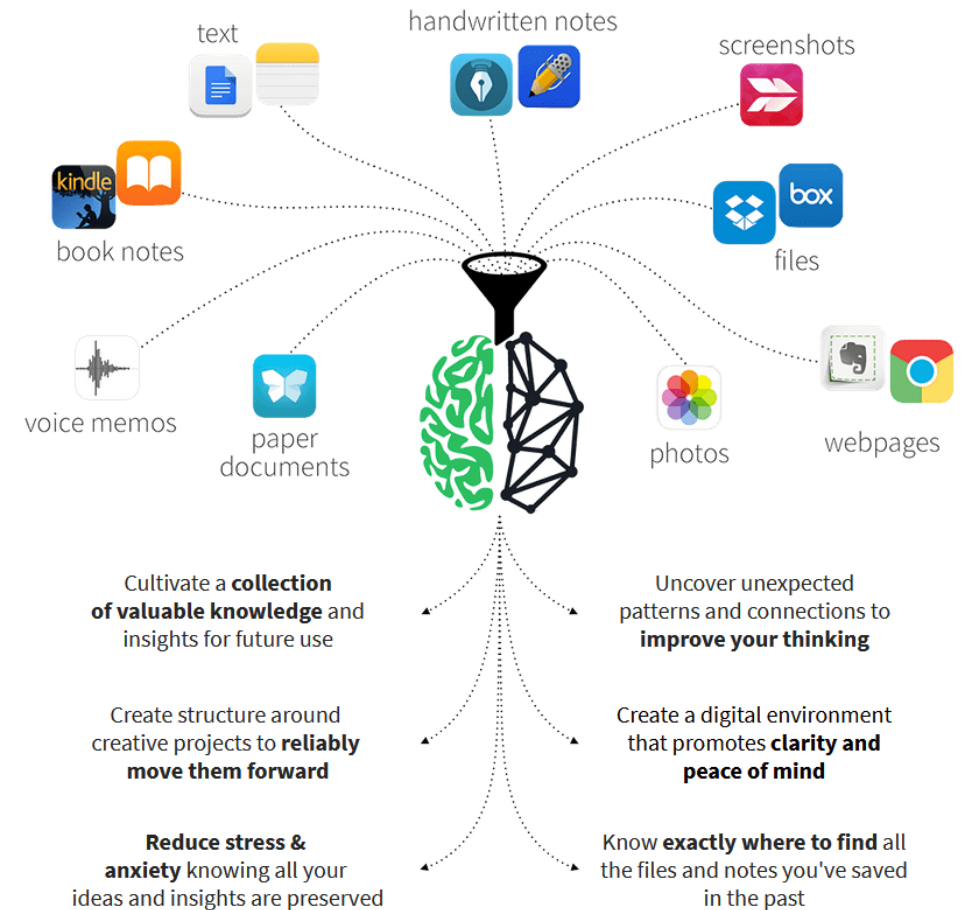
You are going to need a 2nd brain!



2ND BRAIN

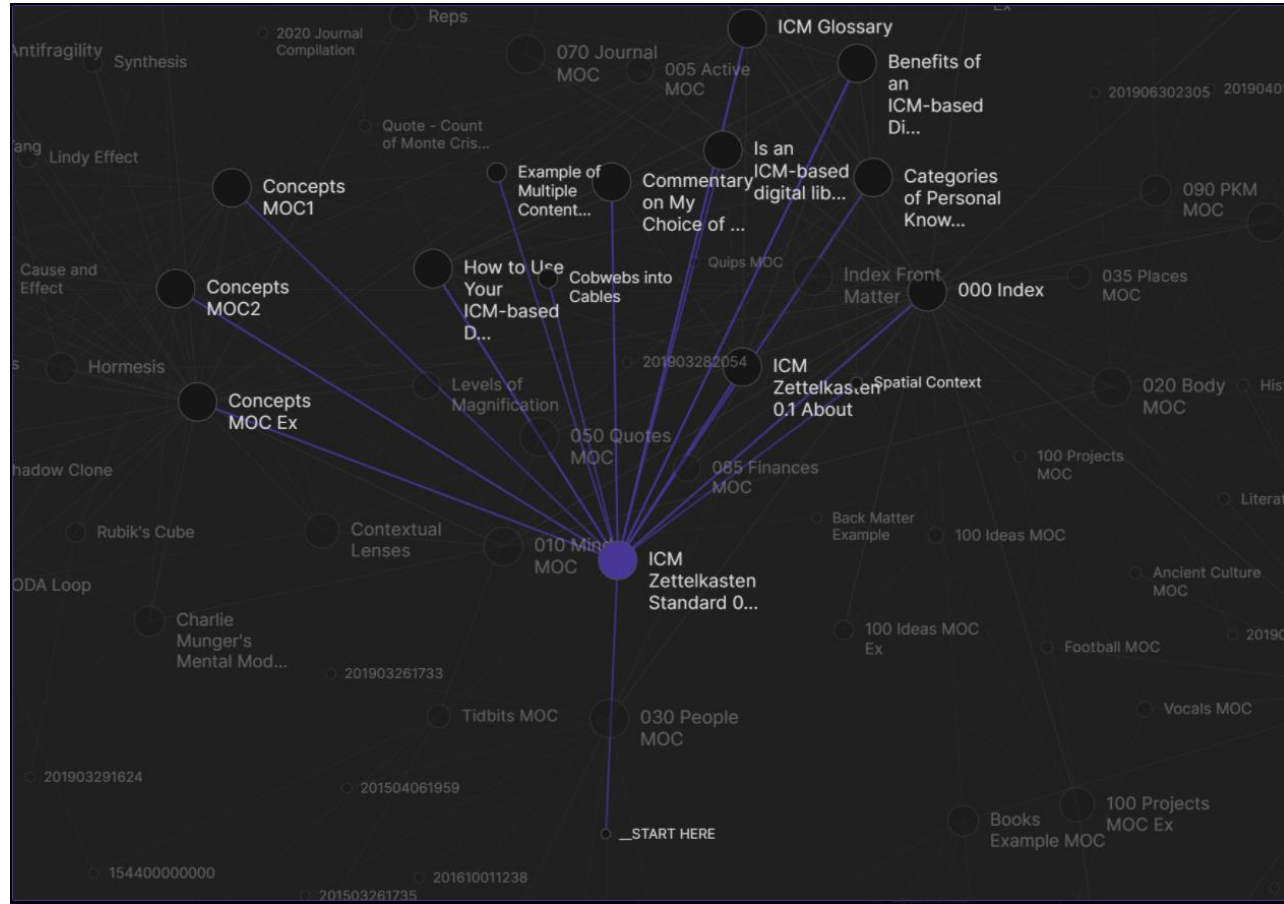
The idea is that we consume so much information everyday that we simply cannot remember it all...

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!

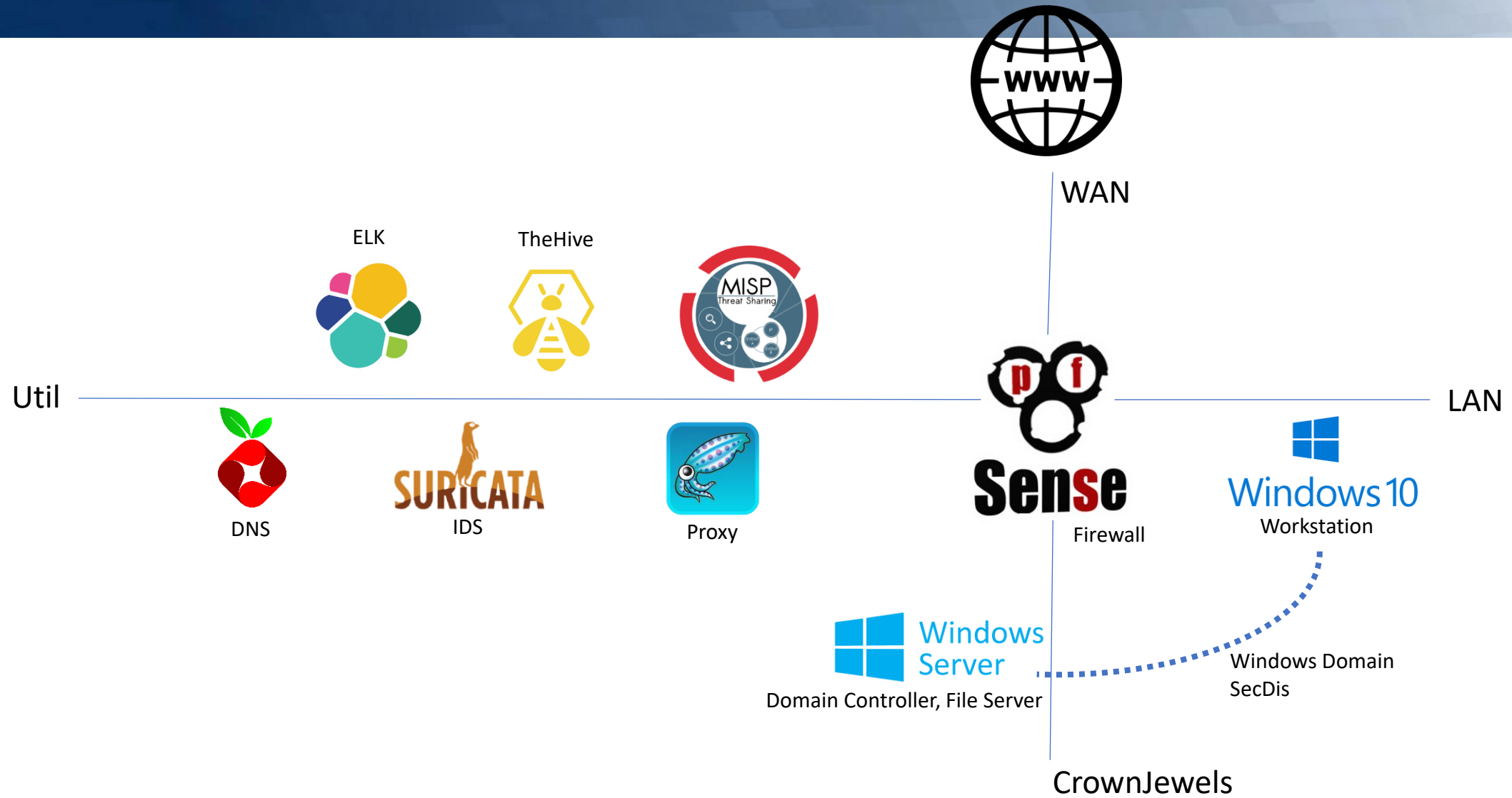
Chapter 3

Having your own Lab

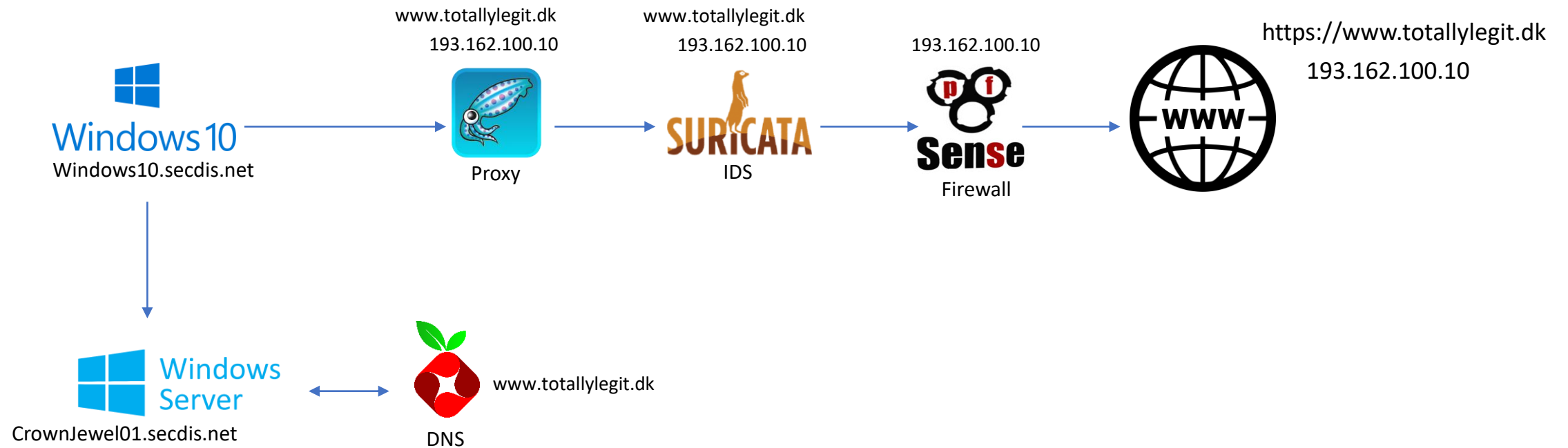
- Saga Lab
- Saga Lab – In practice
- Saga Lab – Logging experience
- Having your own lab



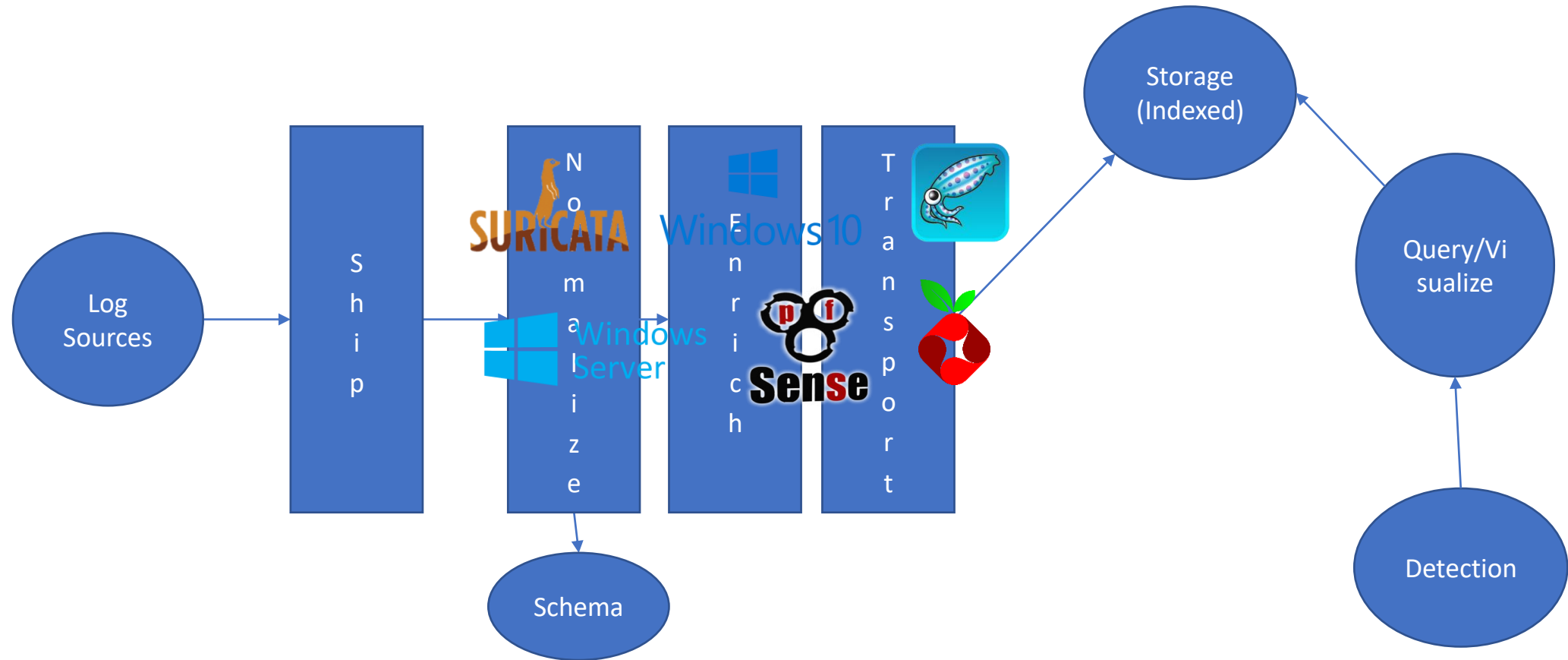
SAGA LAB



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

