

# Langlopende Taak: Deelopdracht deel 1

## Thema: Cybersecurity

Cybersecurity is de praktijk van het beschermen van systemen, netwerken en programma's tegen digitale aanvallen. Deze cyberaanvallen zijn meestal gericht op: het verkrijgen van toegang, het wijzigen of het vernietigen van gevoelige informatie; geld afpersen van gebruikers via ransomware; of het onderbreken van normale bedrijfsprocessen.

### Diensten:

#### Scannen op kwetsbaarheden:



In cybersecurity is het belangrijk om preventief te werken, daarom is het belangrijk om regelmatig een systeem of netwerk te scannen op kwetsbaarheden.

Door te kwetsbaarheden vroeg op te sporen en op te lossen voorkomen we dat ze uitgebuit worden voordat de beheerders van het systeem ervan op de hoogte zijn.

#### Data encryptie:

Data encryptie vertaalt de “plaintext” die we over netwerken versturen naar “cypher-tekst”. Hierdoor wordt de data die verstuurt wordt onleesbaar voor degenen zij die niet de juiste encryptiesleutel hebben. Data encryptie ligt aan de basis van het beschermen van persoonlijke data op het internet. Zeker als je een bedrijf bent dat de persoonlijke data van klanten beheert is het belangrijk om gebruik te maken van data encryptie.



#### Firewall:

Een firewall is een cybersecurity system dat inkomend en uitgaand netwerkverkeer monitort en controleert op basis van op voorhand bepaalde parameters.



Firewalls zijn al meer dan 20 jaar de eerste linie van cyber beveiliging, het is een soort muur tussen je veilig interne netwerk en vreemde netwerken waar je geen controle over hebt. Er zijn veel verschillende soorten Firewalls omdat ze al zo lang bestaan, het is dus belangrijk dat je de juiste soort firewall kiest voor de situatie.

## Endpoint security:

Endpoint security zijn diensten die computers, servers en andere apparaten die met het netwerk verbinden beschermen van cyber aanvallen. Het is belangrijk om een vorm van beveiliging te hebben op elke laag van het netwerk.

Elk endpoint van een netwerk is een mogelijke ingang voor iemand met slechte bedoeling daarom maken grote bedrijven gebruik van Endpoint security.



## Incident response:

In cybersecurity proberen we zoveel mogelijk preventief werk te doen, maar je moet ook kunnen reageren wanneer je beveiliging faalt.

Het proces gaat als volgt: Het begint met **voorbereiding**, wanneer er geen huidige problemen zijn binnen het netwerk moet het security team nog steeds voorbereidend werk doen. De volgende stap is **detectie en analyse** van je netwerk, je kan cyber security problemen alleen maar oplossen als je ze eerst vindt. Daarom is het belangrijk om je netwerk goed te monitoren of hier een security solution voor in te zetten. Als je een beveiligingsprobleem binnen je netwerk hebt gevonden proberen we het eerst **af te sluiten** van de rest van het netwerk en zo de dreiging te minimaliseren. Nu we zeker zijn dat het probleem zich niet verder zal verspreiden is het tijd om het van ons netwerk te **verwijderen**.

Bijvoorbeeld malware binnen een systeem vernietigen of een ongewenste gebruiker kicken. Het probleem is vernietigd dus de volgende stap is de schade die is aangericht **herstellen**. Bijvoorbeeld nieuwe securitypatches uitbrengen of data herstellen met behulp van back-ups. Een van de belangrijkste stappen van het proces komt nadat het probleem opgelost is: de **post incident review**.

De leden van het security team of de dienst die je netwerk beschermt gaan na een incident grondig nakijken hoe het incident is gebeurd, om er dan voor te zorgen dat er zich geen soortgelijke breach kan voordoen in het systeem (Soms word er ook een statement gemaakt bv wanneer mensen hun persoonlijke data in gevaar werd gebracht).



## Penetratie testen:

Een goeie gewoonte is om af en toe je eigen systeem/netwerk te testen. Hiervoor huur je een bedrijf in dat een gesimuleerde cyberaanval zal uitvoeren op je servers, dit is een van de beste manieren om kwetsbaarheden in je systeem te vinden. Dit wordt vaak gedaan door “ethische hackers” zij weten hoe ze netwerken kunnen binnen geraken maar gebruiken hun kennis voor goede doeleinden en helpen er bedrijven mee. Vaak zul je ook een gedetailleerde analyse krijgen van de kwetsbaarheden binnen je systeem.



## Soortgelijke Websites

(Kijk achteraan het document voor de printscreens van de websites)

<https://cybermap.kaspersky.com/stats> : Het dashboard van deze website spreekt mij aan door het kleurpalet. De kleuren die gebruikt worden om de data weer te geven steken duidelijk af tegen de achtergrond. Het dashboard is ook vrij interactief je kan kiezen welke data er getoond word en welke niet.

<https://www.criminalip.io/intelligence/statistics> : Dit dashboard is minimalistisch en is iets minder interactief. De data word op een vrij saaie manier weergegeven, het kleurpalet is zacht voor de ogen en zorgt voor een overzichtelijke site.

<https://exchange.xforce.ibmcloud.com/> : Dit dashboard vond ik eerst een beetje druk er sprongen veel dingen in het oog wat overweldigend was. Het kleurenpalet lijkt op een standaard dark-mode met wat pastel kleuren in de accenten. Het idee van de verschillende vakjes in je dashboard die al data tonen waar je op kan doorklikken vind ik wel goed, persoonlijk zou ik de data die word getoond nog een beetje minimalistische of ordelijker weergeven

<https://threatmap.checkpoint.com/> : Dit dashboard toont een interactieve live cyber threat map, we zien dat de hoofdzakelijke kleuren donker zijn en er worden felle kleuren gebruikt voor de details dit vind ik overzichtelijk. Door op een land op de kaart te klikken zie je de data over cyber threats voor dat land deze data word ook overzichtelijk weergegeven.

<https://www.paloaltonetworks.com/resources> : De resources pagina van deze site heeft een klein minimalistisch dashboard waar de gebruiker cyber security data kan vinden. Er kan gefilterd worden op medium maar ook op sector, onderwerp, datum van uitgave enz. Het kleurenpalet is niets speciaal maar het oogt wel ordelijk en overzichtelijk.

## Kleurenpalet

Hoofdkleur : #089103

Complementair: #CC0472

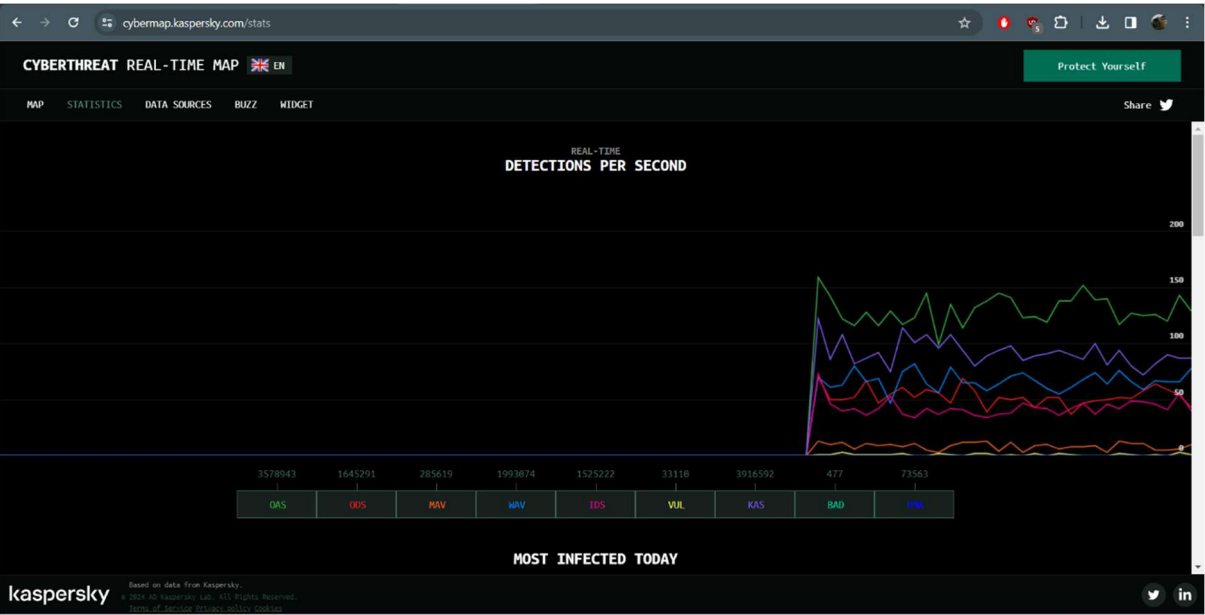
Details: #A5E887

## Voorlopig logo



# Printscreens

Cybermap.kaspersky:

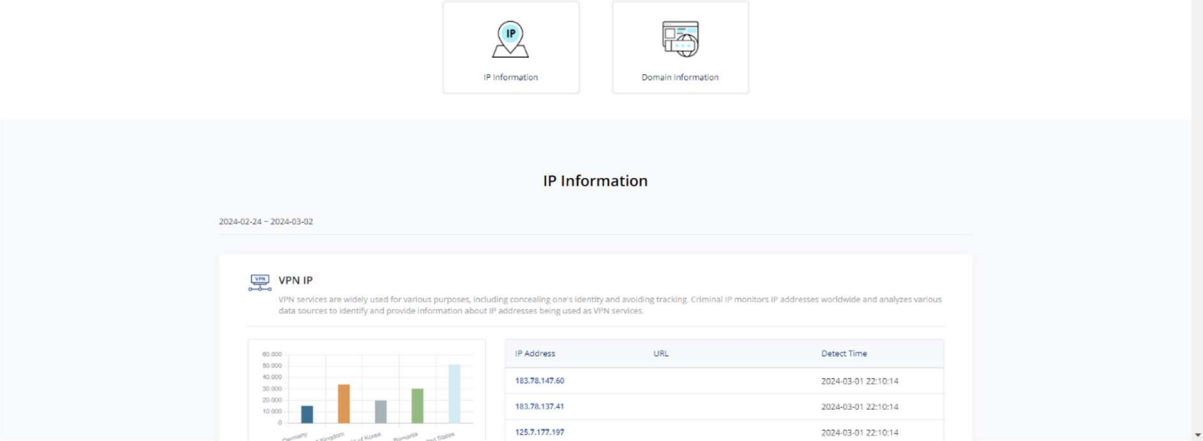
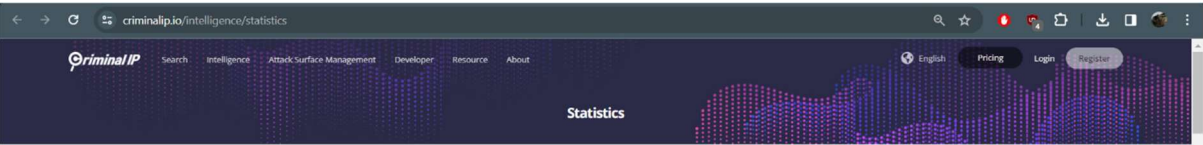


On-Access Scan

TIME PERIOD: Last week Last month

WORLD	North America	South America
1 Guinea-Bissau 8.99%	1 Nicaragua 4.89%	1 Bolivia 5.35%
2 Myanmar 8.79%	2 Cuba 4.81%	2 Venezuela 4.48%
3 Afghanistan 8.79%	3 Honduras 2.9%	3 Brazil 3.7%
4 Turkmenistan 8.38%	4 Guatemala 2.86%	4 Ecuador 3.39%
5 Benin 8.15%	5 Mexico 2.84%	5 Peru 3.08%
6 Burundi 7.86%		
7 Cameroon 7.78%	Asia	Europe
8 Congo Republic 7.64%	1 Myanmar 8.79%	1 Belarus 4.87%
9 Togo 7.64%	2 Afghanistan 8.79%	2 Moldova 4.72%
10 Rwanda 7.34%	3 Turkmenistan 8.38%	3 Russia 4.14%
11 Angola 7.25%	4 Bangladesh 6.69%	4 Poland 3.24%
12 Burkina Faso 7.18%	5 Laos 6.68%	5 San Marino 3.18%
13 Tanzania 7.17%		
14 Guinea 7.81%	Africa	Oceania
15 Central African Republic 6.91%	1 Guinea-Bissau 8.99%	1 Fiji 2.44%
16 Mozambique 6.91%	2 Benin 8.15%	2 Maldives 2.07%
17 Côte d'Ivoire 6.79%	3 Burundi 7.86%	3 New Caledonia 2.07%
18 Mali 6.73%		

Criminalip:

This screenshot shows the 'Domain Information' section of the CriminalIP website. It features a date range '2024-03-01 ~ 2024-03-02'. The section is divided into four sub-sections: 'Malicious Domain', 'VPN Domain', 'Phishing Domain', and 'Recent Domain'. Each sub-section contains a table of detected domains, URLs, IP addresses, and detection times.

Malicious Domain	
URL	Detect Time
https://netflix-clone-5066d.web.app	2024-03-01 22:59:07
http://saamlas-netflix.com	2024-03-01 22:58:06
http://a-simple-netflix-clone.vercel.app	2024-03-01 22:57:04
http://netflix-landing-page-vi.vercel.app	2024-03-01 22:56:03
http://171.39.201.244:52148/Mozl.m	2024-03-01 22:55:11

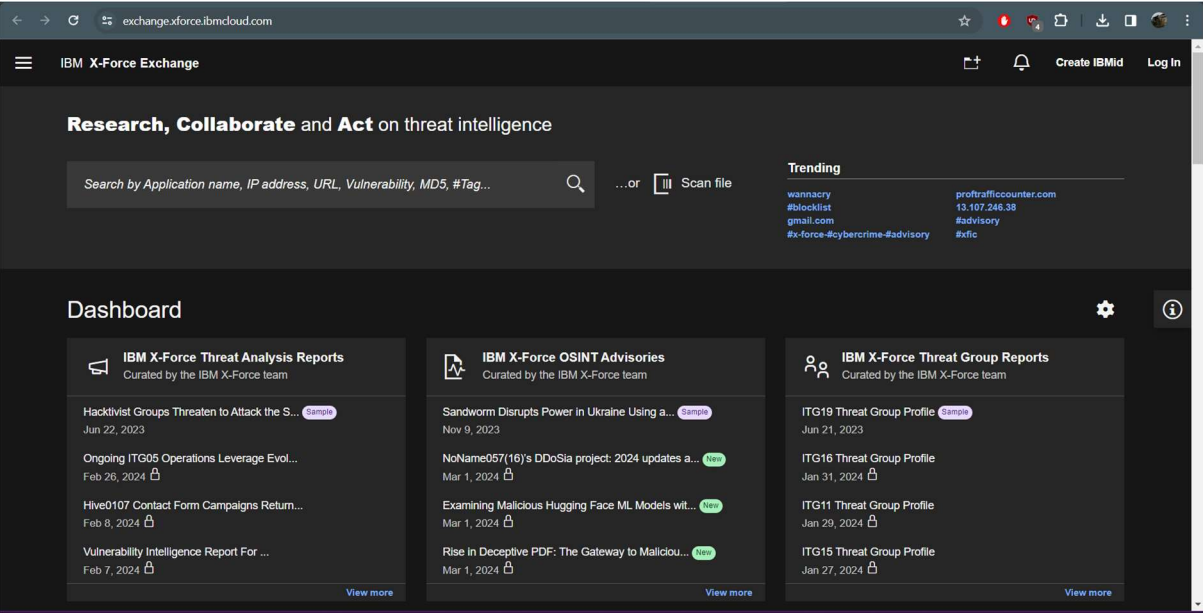
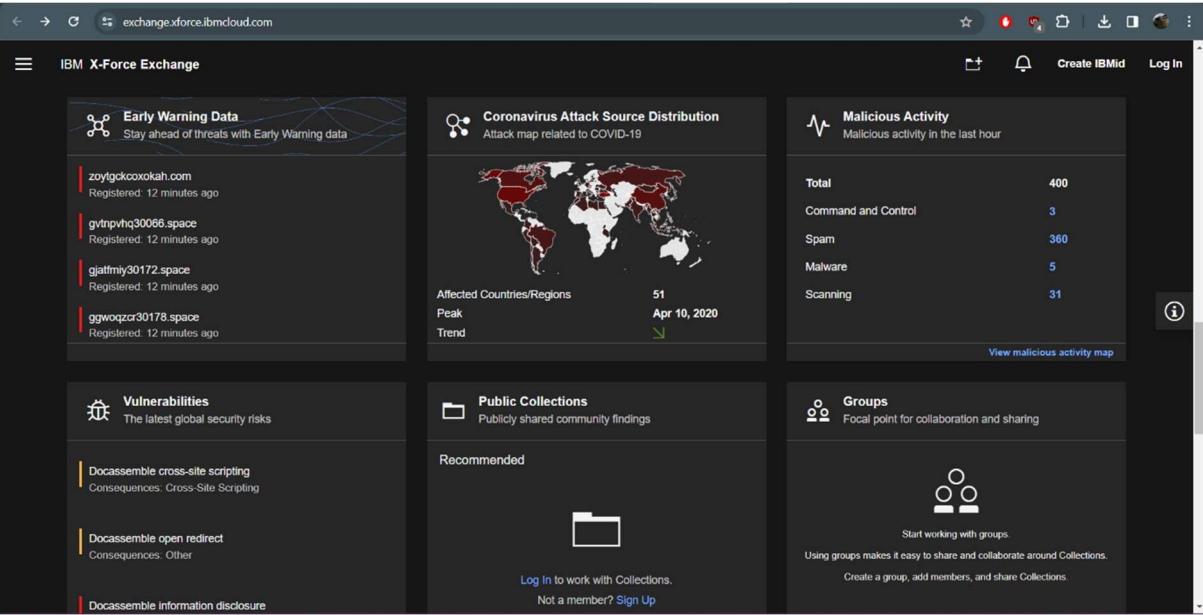
VPN Domain	
URL	Detect Time
vpn700578812.opengw.net	2024-03-01 21:20:36
vpn597615796.opengw.net	2024-03-01 21:20:36
public-vpn-135.opengw.net	2024-03-01 21:20:36
vpn393914289.opengw.net	2024-03-01 21:20:36
vpn309270657.opengw.net	2024-03-01 21:20:37

Phishing Domain	
URL	Detect Time
http://171.39.201.244:52148/Mozl.m	2024-03-01 22:55:11
http://netflix-landing-page-vi.vercel.app	2024-03-01 22:56:03
http://a-simple-netflix-clone.vercel.app	2024-03-01 22:57:04
http://saamlas-netflix.com	2024-03-01 22:58:06
https://netflix-clone-5066d.web.app	2024-03-01 22:59:07

Recent Domain		
URL	IP Address	Detect Time
jakob-studios.com	162.55.180.176	2024-03-01 17:34:14
countynp.com	198.49.23.144	2024-03-01 17:34:19
90bz7c5a.baby	137.220.183.163	2024-03-01 17:34:36
juice-bet.com	104.21.42.196	2024-03-01 17:34:37
bremasamerica.pro	15.197.148.33	2024-03-01 17:34:38

Self-signed Domain	
URL	Detect Time

Exchangeforce.ibm:





## Checkpoint threatmap:





## Paloaltonetworks:

← → ↻ [paloaltonetworks.com/resources](#) 🔍 ☆ 📄 📄 📄 📄 📄 📄

PRESS RELEASE  
(886)

VIDEOS  
(176)

DATASHEET  
(136)

WHITEPAPERS  
(162)

WEBINAR  
(104)

CUSTOMER STORY  
(288)

SOLUTION BRIEFING  
(23)

NGFW  
(141)

PRISMA CLOUD  
(408)

CORTEX XDR  
(138)

CORTEX XSIAM  
(39)

CORTEX XDR  
(218)

FINANCIAL SERVICES  
(79)

MANUFACTURING  
(14)

Displaying 1-16 of 7097

Sort by: Newest ▾

Date ▾

Topic ▾

Industry ▾

Products ▾

Services ▾

Type ▾

Educational and Professional Services ▾

**203% three-year ROI**  
The value of platformization

[Learn more](#)

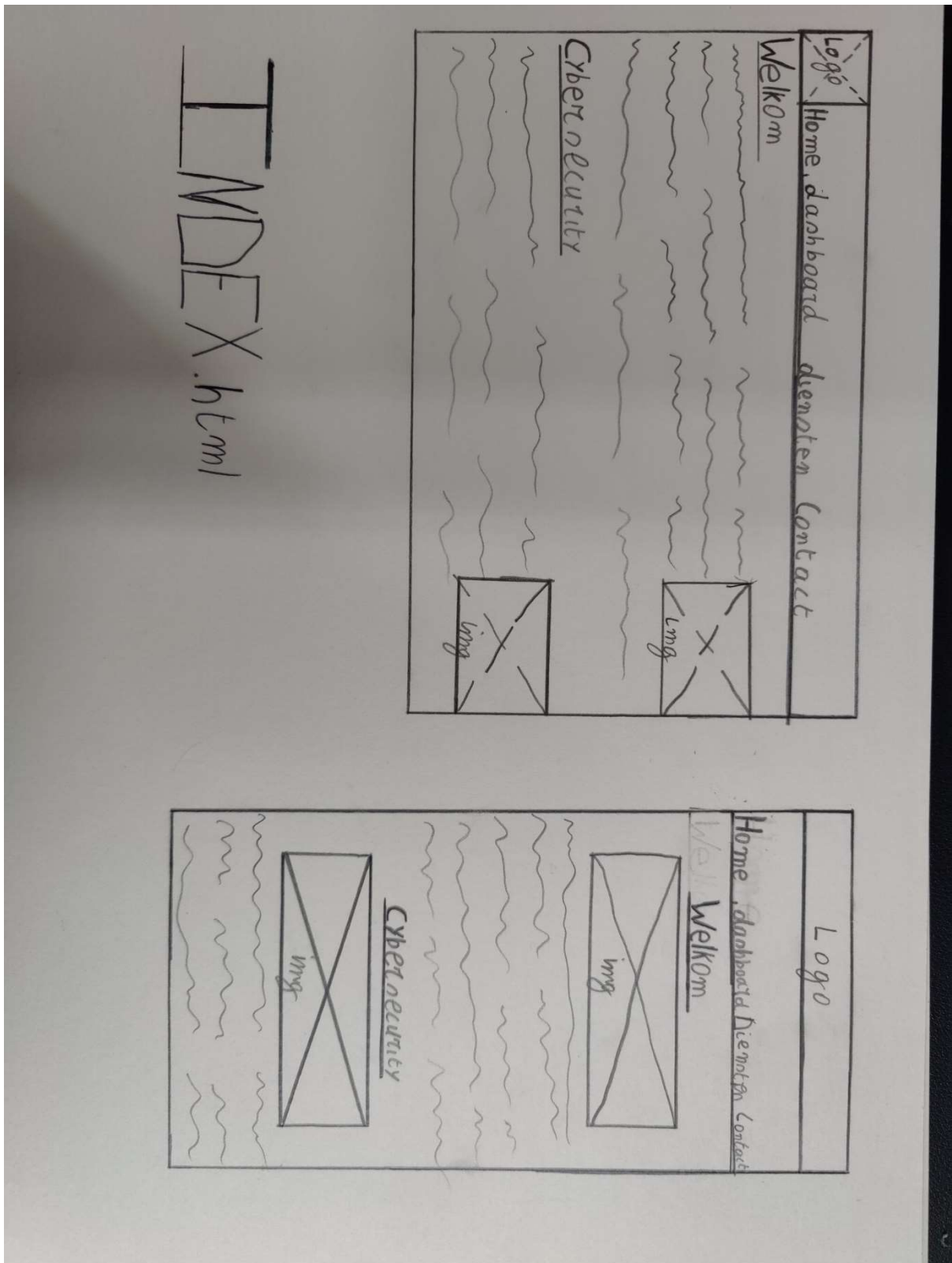
**UNIT 42**  
**Wireshark Tutorial:**  
Exporting Objects From a Pcap

[Read the story](#)

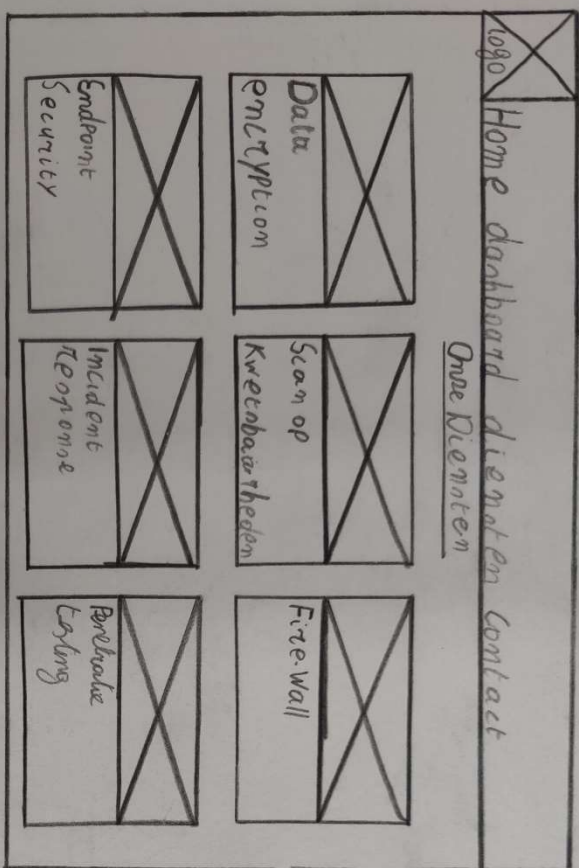
## Langlopende taak: deelopdracht 2

Wireframes:

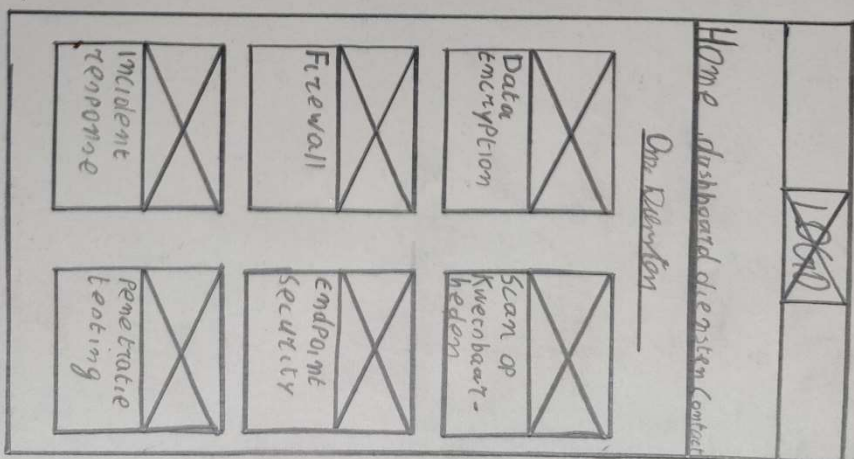
Index.html:

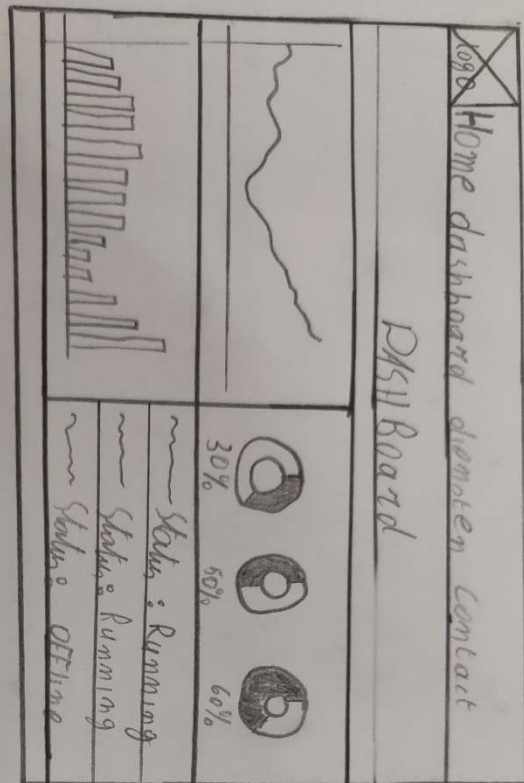


Diensten.html:

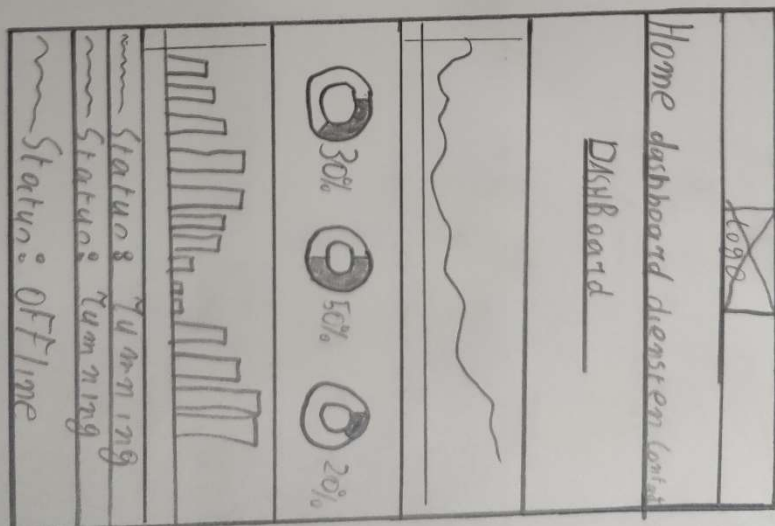





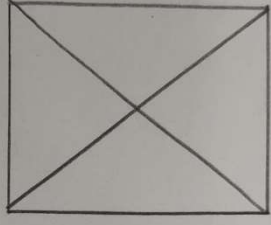
D I E N S T E N . h t m l





DASHBOARD.html



logo	Home Dashboard Register Contact
<u>Contact</u>	
Address: ~ ~ ~ ~ ~	
Telephone: +32 ~ ~ ~ ~ ~	
Email: ~ ~ ~ ~ ~@ ~ ~ ~ ~ ~	
Socials	
  	

Contact.html

	logo	
Home Dashboard Register Contact		
<u>Contact</u>		
Address: ~ ~ ~ ~ ~		
Telephone: +32 ~ ~ ~ ~ ~		
Email: ~ ~ ~ ~ ~@ ~ ~ ~ ~ ~		
Socials		
