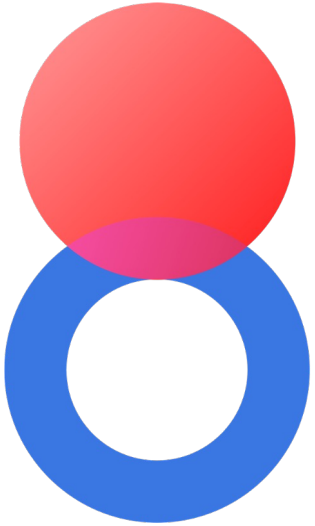
Praktische Purple Teaming

FalconForce

Together. Secure. Today.



Chapter 8

We Train Your Defenders

22 november 2022 - PvIB

Programma

- Wie?
- Context

- Wat is Purple Teaming (niet)
- Waarom Purple Teaming?
- …en waarom niet?

- De praktijk

- Bedtime Stories

Pepijn Vissers

Chapter8

healer // co-founder

“de man in pak”

Givan Kolster

@ FalconForce

Purple team lead, project manager, haalt de koffie

- Veel red en purple teaming opdrachten geleid
- Social engineer, je kunt me vertrouwen

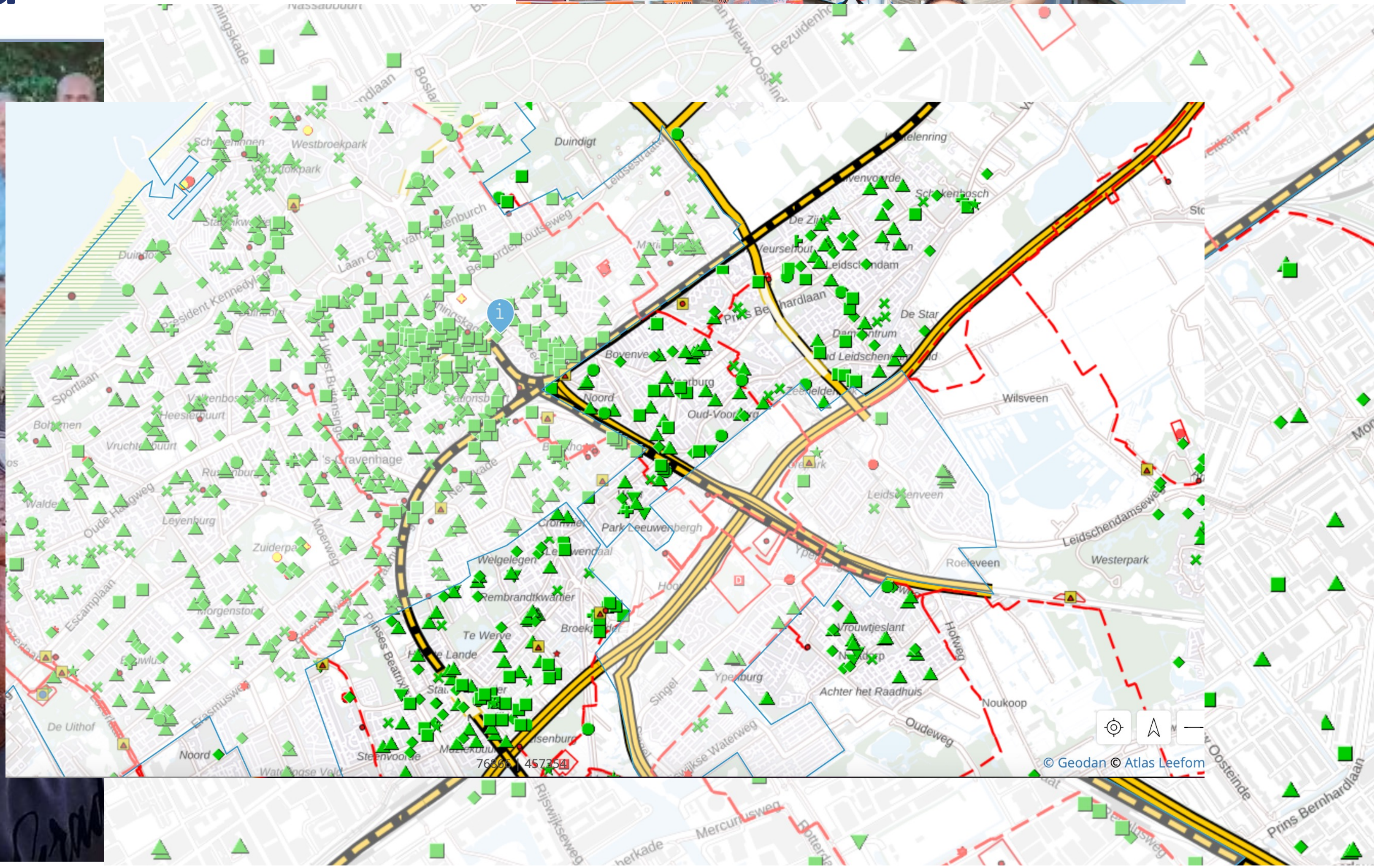
Erg trots op mijn gezin: mijn vrouw en drie kinderen.
Gek op gezonde dingen: hardlopen, plantaardig eten en in de natuur zijn.

linkedin.com/in/givankolster/
medium.com/@givankolster
givan@falconforce.nl
falconforce.nl

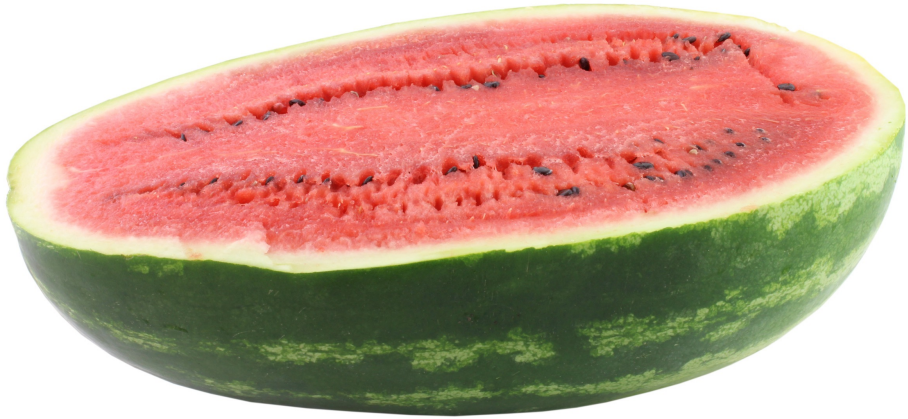
context

IT vroeger

IT nu


Duindigt
Westbroekpark
Scheveningen
's-Gravenhage
Bohemen
Vruchtenbuurt
Waldeck
Leyenburg
Morgenstond
Zuiderpark
De Uithof
Wilsveen
Westerpark
Leidschendamseweg
Leidschenveen
Roeleveen
Noukoop
Oudeweg
Achter het Raadhuis
Vrouwtjeslant
Ypenburg
Rembrandtkwartier
Welgelegen
Te Werve
Park Leeuwenbergh
Oud-Voorburg
De Star
Prins Bernhardlaan
Laan Copes van Cattenburch
Steenvoorde
Rijswijkseweg
Mercuriusweg
Prins Bernhardlaan
© Geodan © Atlas Leefom

de gevolgen



Context

- Organisch gegroeide omgevingen
- Watermeloenen

- Hoe kom je van een watermeloen naar een granaatappel?

- …dit is geen nieuw probleem!

Wat is Purple Teaming (niet)?

Purple teaming is een kans om te leren

Maar dat geldt toch ook voor …

Audits

Vulnerability scanning

Penetration test

Red teaming

Threat led testing (e.g. TIBER, CBEST, ZORRO)

Missen we iets?

Missen we iets?

Waar is de samenwerking?

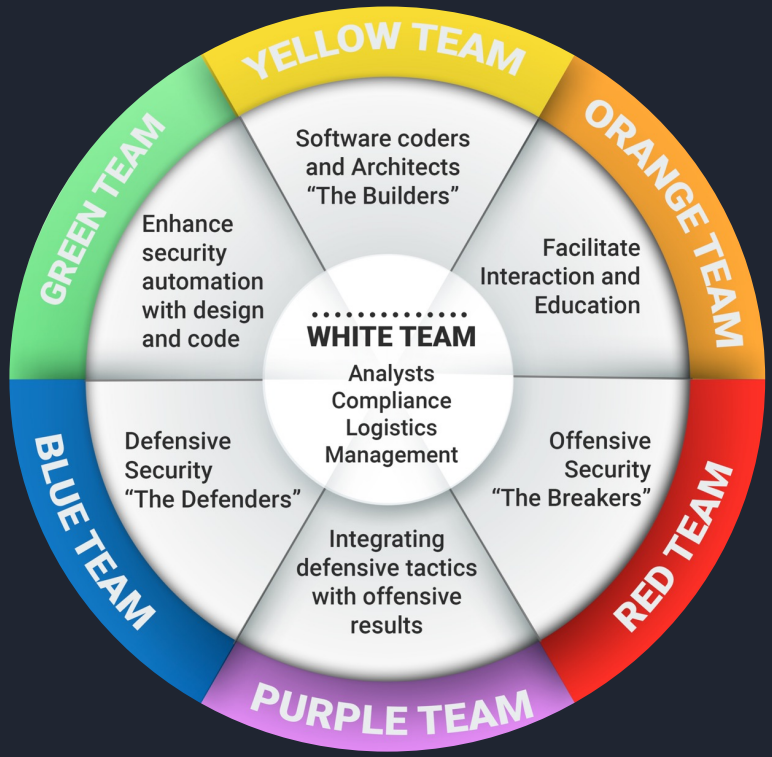

“Organisaties
weerbaar
maken tegen
aanvallers.”

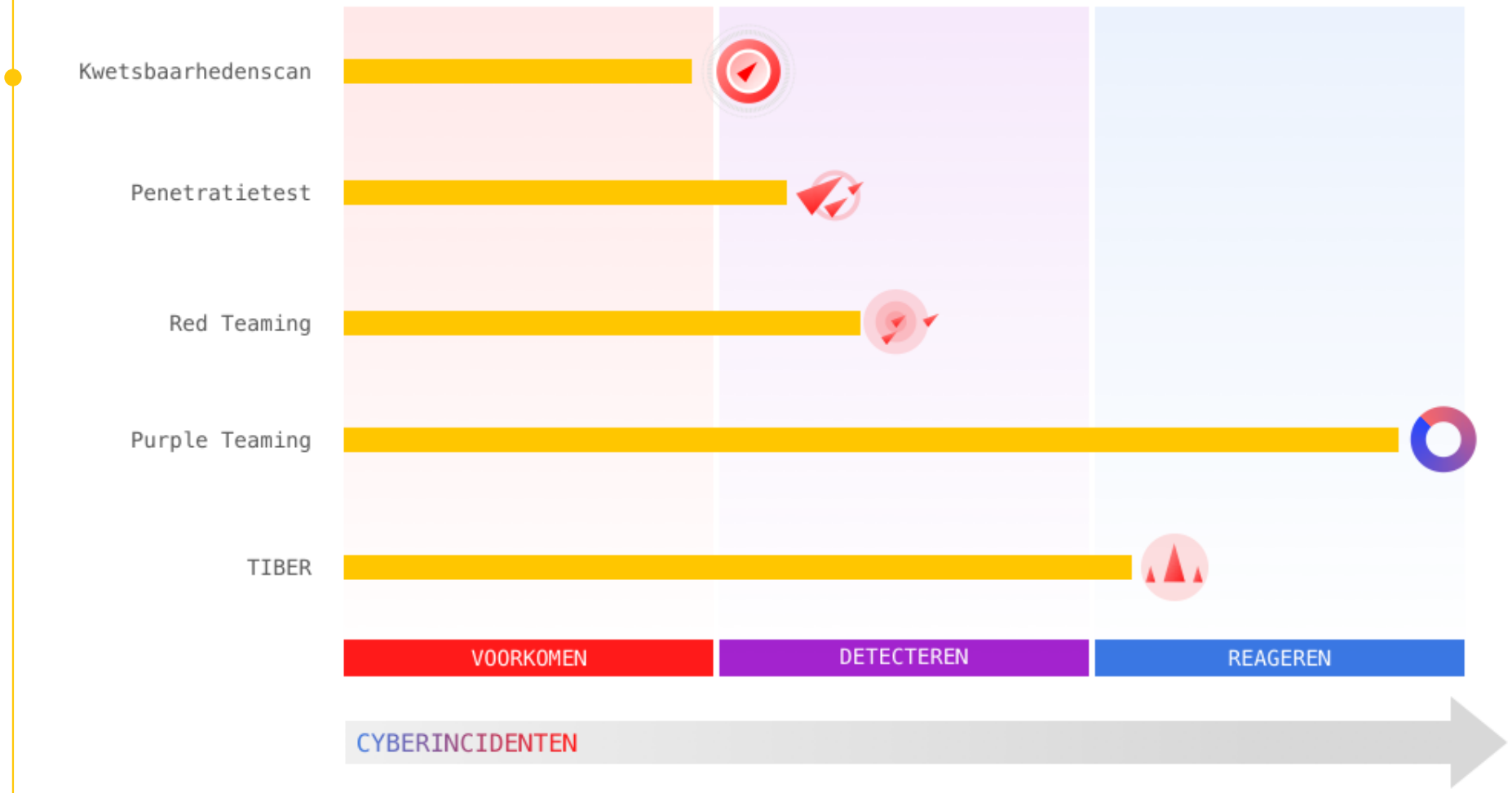
Een shift van “vs.” naar 💜

Red Team, offensief
Blue Team, defensief

Mix ze samen en je krijgt purple.

Samenwerking is essentieel!

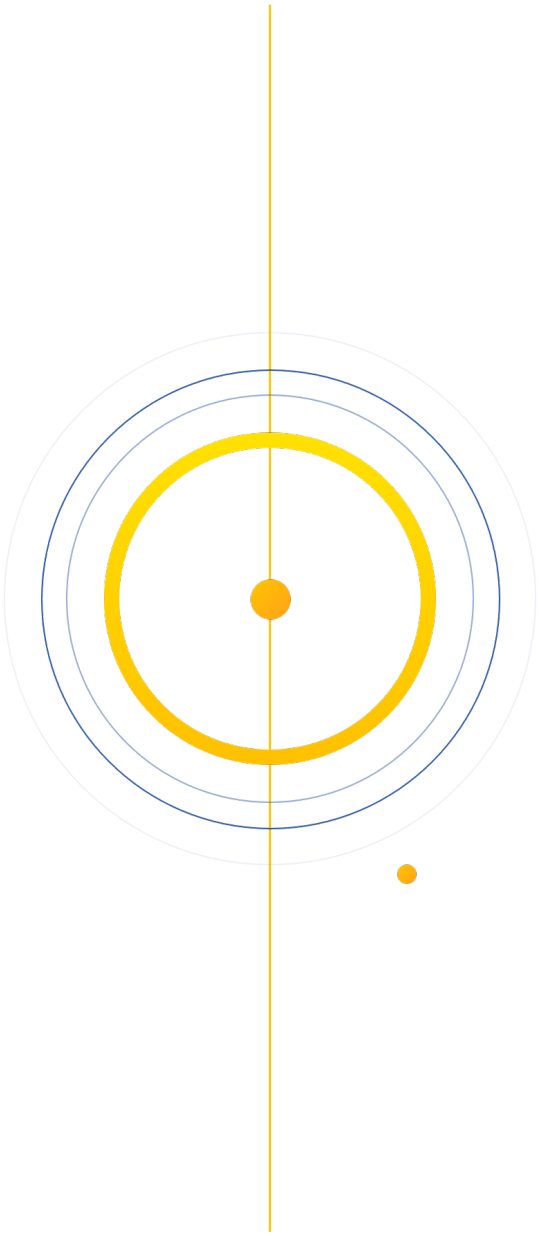



Kwetsbaarhedenscan
Penetratietest
Red Teaming
Purple Teaming
TIBER
VOORKOMEN
DETECTEREN
REAGEREN
CYBERINCIDENTEN

Kernprincipes
Purple Teaming

Principe 1: kroonjuwelen

- **dingen die pijn doen bij schade**
  - “reputatie"
  - “intellectueel eigendom”
  - “gevoelige informatie”
  - “niet kunnen werken”



Principe 1: kroonjuwelen

- ***tastbare* dingen die pijn doen bij schade**
  - gedetailleerde blauwdrukken
  - onze nieuwe technologie, Q
  - persoonsgegevens
  - kritieke systemen

Principe 2: Assume breach

Principe 3: Train as they fight

Samenvatting Purple Teaming

- Kroonjuwelen +
- Assume breach +
- Train as they fight =

- “as real as it gets”
- een cybercrisis-simulatie

- overt vs covert (?)

Waarom zou je Purple Teaming überhaupt willen?

“She loves me”

Kans om te ”winnen” voor het blue team

Er is EINDELIJK een naald in de hooiberg te vinden.

Training-on-the-job

Team building

Oefening baart kunst

“She loves me not”

Kosten

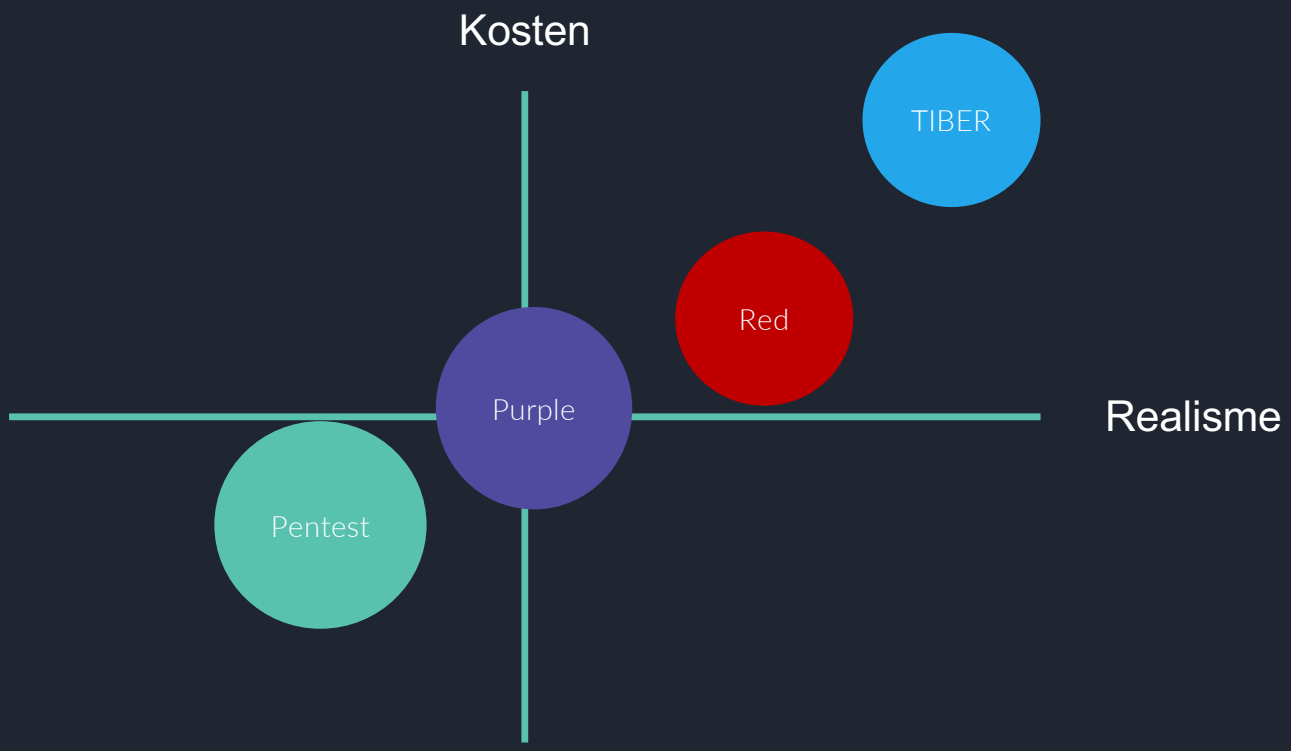
Bezetting van het blue team

Iedereen is op de hoogte, realisme gaat omlaag

Lage volwassenheid van de eigen organisatie

Wanneer overwegen we purple teaming?

Wanneer overwegen we purple teaming?

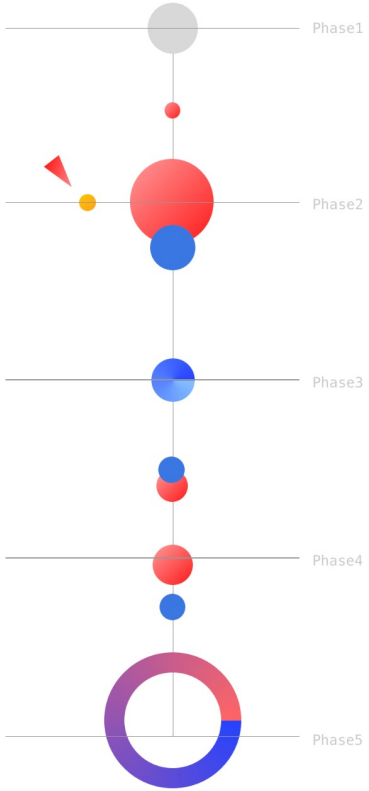


#hoedan

#hoedan

Intake

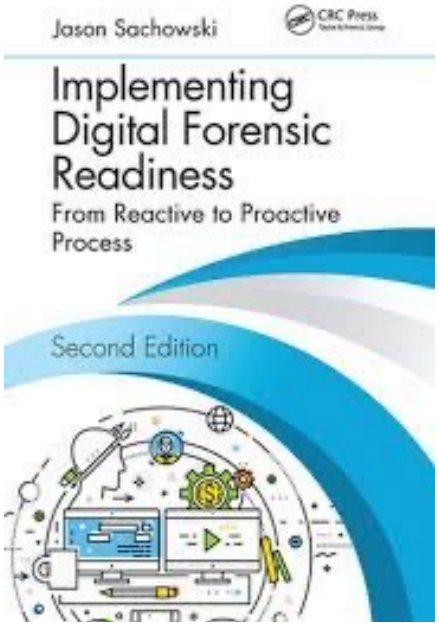
- strategisch: stakeholders aan tafel!
- tactisch: kroonjuwelen
  scope (??)
- operationeel: startpunten,
  logging en monitoring
- succes wanneer

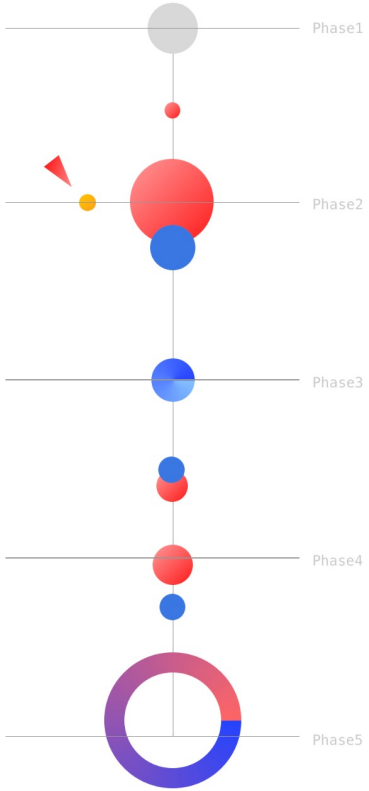


#hoedan

Verkenning / analyse

- documenteer! (VECTR.io)
- communiceer! (Signal / Mattermost)
- pas niveau aan
- geen paniek
- GEEN MAJOR CHANGES tijdens uitvoering
- hoe reageert de organisatie?

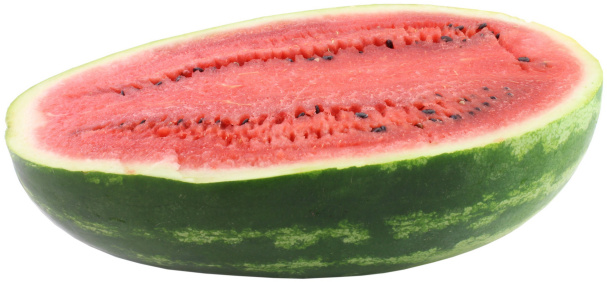




#hoedan

Rapportage

- Meerdere presentaties (…meestal)
- Niet vingerwijzen
- Plannen maken richting een beter *Verdedigbaar Netwerk*
- …of de FalconForce aanpak



Samen verschillen

Verschillen in aanpak

Chapter8

Procesfocus

Ontwikkellen en finetunen IR proces

Laag tot medium volwassenheid SOC

AIVD *Verdedigbaar Netwerk*

FalconForce

Technische focus

Ontwikkelen en finetunen detecties

Medium tot hoog volwasenheid SOC

MITRE ATT&CK

Bedtime stories

Er was eens …

What-if scenario's: wat als het volgende zich voordoet?

Table-top

Moderator

Lessons learned

Proces(documentatie) beschikbaar

Blind-spots in het proces zichtbaar

Direct incidenten aangemaakt

"Laten we dit vaker doen"

Van donkerrood…

“Wat was dat wachtwoord ook al weer…?”

- ⟶ **Implant**
- ⟶ **Goedemorgen!: Domain Admin vlak na de lunch**
- ⟶ ***But why stop there***

- ⟶ **Administrator@ als service account**
- ⟶ **Sterk wachtwoordbeleid,**
- ⟶ NIET afgedwongen

“Wat was dat wachtwoord ook al weer…?”

…naar kobaltblauw

jaaaaa

@channel

		AutoPilotDeploy	Enabled	513	
	36	Pim [redacted]	Enabled	513	
	16	Nick [redacted]	Enabled	513	
		svcin [redacted]	Enabled	513	pw = 2mhnao!SGXF8i
	36	Hana [redacted]	Enabled	513	
	43	Arthu [redacted]	Enabled	513	
	0	Rob [redacted]	Enabled	513	
	4	Natas [redacted]	Enabled	513	

janwillem 10:29 PM

username/password incorrect....man!

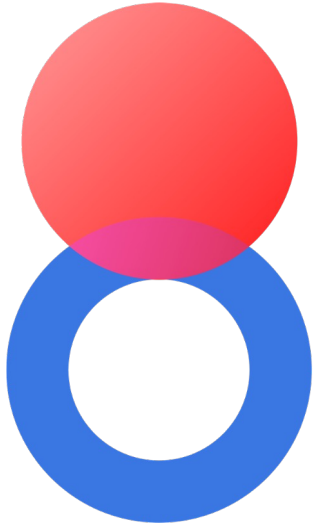

HOC PROBAMUS
CHAPTER 8


ASK

Bedankt voor jullie aandacht!

FalconForce

Together. Secure. Today.



Chapter 8

pepijn@chapter8.com – Pepijn Vissers, MSc
givan@falconforce.nl – Givan Kolster