HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES

De dag dat je gehackt wordt

MATTIJS DIJKSTRA

Inhoudsopgave

VANDAAG DE DAG

Dreigingslandschap

Gehackt

In de praktijk

..Wat nu

HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES

Dreigingslandschap Maritieme Sector

PUBLIC

Trends

MARITIEME SECTOR

Industry 4.0

- Ontwikkelingen zoals Big Data, Artificial Intelligence and Autonome technologie worden steeds meer toegepast
- Information Technology (IT) en Operation Technology (OT) systemen zijn meer en meer geïntegreerd > schepen zijn meer verbonden dan ooit
- Ontwikkelingen vergroten aanvalsoppervlak > evenals potentiële impact

Duurzaamheid

- R&D was noodzakelijk om ambitieuze duurzaamheids doelstellingen te realiseren in de industrie
- Race om de meest (kosten) efficiente manier te vinden om uitstoot te verminderen
- APTs ingezet door verschillende staten om het kostbare R&D process te omzeilen door middel van informatie dierstal en spionage

Weerbaarheid

- Wereldwijde systemen kwetsbaar voor supply chain aanvallen
- Ransomware kan significante impact hebben op operationele continuïteit
- Complex dreigingslandschap met verschillende actoren > piraten, terroristen, cyber/ransomware groepen en nation states

CASE 1

Ransomware attack op Royal Dirkzwager

Tijdlijn:

- Ransomware attack gedetecteerd op **6 Maart 2023**.
- Systemen direct offline gehaald, en sommige diensten meer dan een week offline
- Op 16 Maart is 16,5GB gepubliceerd op het dark web, en er werd gedreigd meer te publiceren tenzij betaald zou worden
- Persoonlijke en privé data gepubliceerd op een dark web forum, waaronder contract informatie, paspoorten, werknemer informatie, en meer.

Aanvaller: Play Ransomware Groep (Rusland gelieerd)

Motivatie: Financieel

Impact: Data lek, significante operationele disruptie

CASE 2

Russische DDoS aanval op NED havens

Tijdlijn:

- DDoS aanval tegen websites van meerdere Nederlandse havens in Juni 2023, resulterend in onbereikbaarheid van meerder websites. Getroffen havens zijn Rotterdam, Amsterdam, en Den Helder.
- Twee weken later, website van Noordzee Haven, met havens in Vlissingen, Terneuzen en Gent, was doelwit

Aanvaller: NoName057(16)

Relaties: Rusland gelieerde hacktivisme groep die actief is geworden na de Russische inval in Oekraïne

Impact: Beperkte disruptie

Motivatie: Vergelding nadat de Nederlands overheid heeft aangekondigd de intentie te hebben om Zwitserse tanks aan te schaffen voor Oekraïne

CASE 3

Rederijen geïnfecteerd met Chinese malware

Tijdlijn:

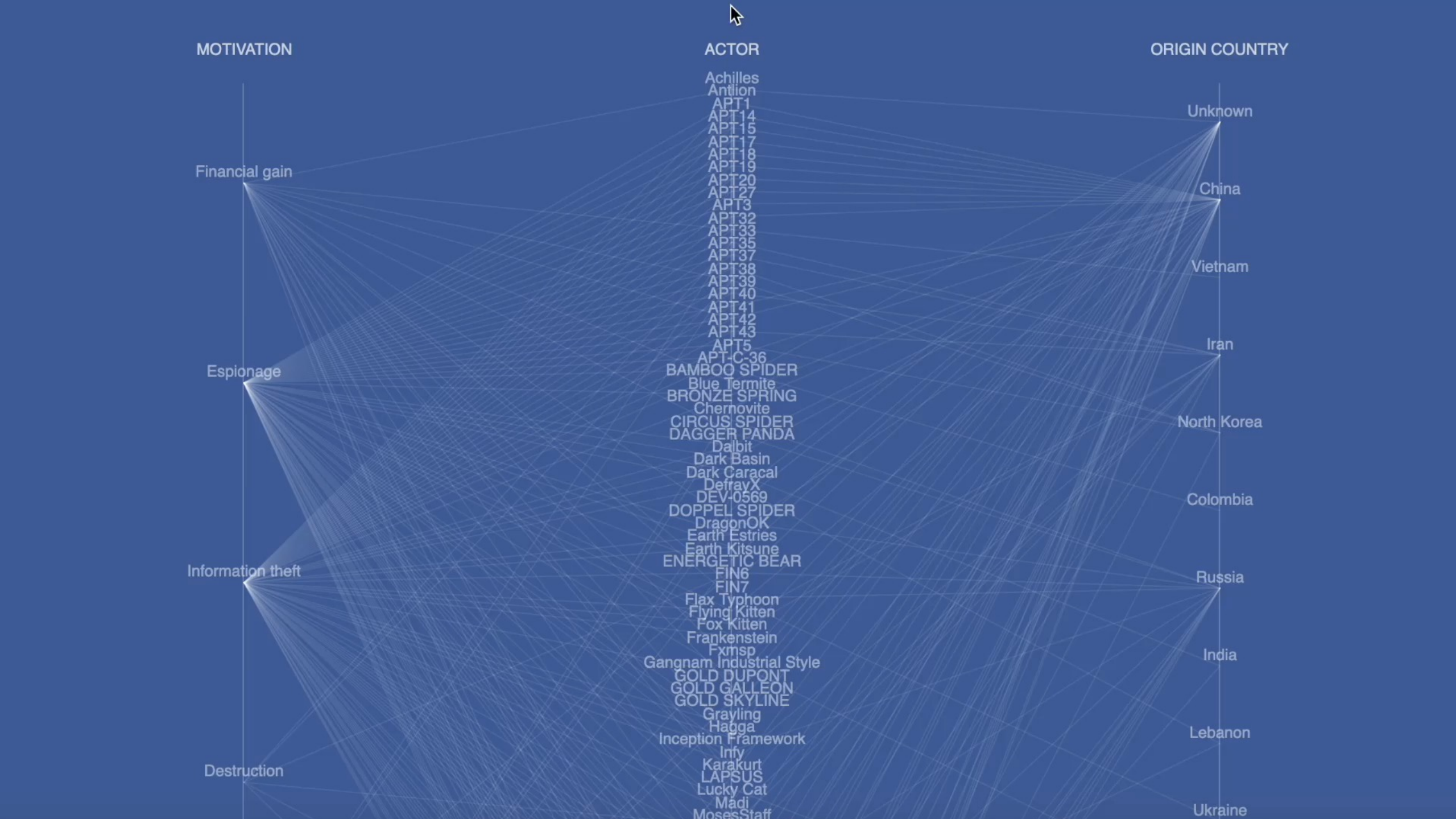
- **Mei 2024:** Malware aangetroffen op systemen van commerciële rederijen in Griekenland, Noorwegen en Nederland, inclusief op systemen op schepen.
- Korplug RAT gebruikt om commando's uit te voeren en informatie te verzamelen over (slachtoffer) systemen
- Malware in sommige gevallen via USB verspreid

Aanvaller: Mustang Panda (China gelieerd)

Motivatie: Spionage

"We haven't seen this in the past...It shows a clear interest in this sector. This was not a single occurrence. These were several distinct attacks at different, unrelated organizations"

- Robert Lipovsky, principal threat intelligence researcher at ESET


MOTIVATION
ACTOR
ORIGIN COUNTRY
Financial gain
Espionage
Information theft
Destruction
Achilles
Antlion
APT1
APT14
APT15
APT17
APT18
APT19
APT20
APT27
APT3
APT32
APT33
APT35
APT37
APT38
APT39
APT40
APT41
APT42
APT43
APT5
APT-C-36
BAMBOO SPIDER
Blue Termite
BRONZE SPRING
Chernovite
CIRCUS SPIDER
DAGGER PANDA
Dalbit
Dark Basin
Dark Caracal
DefrayX
DEV-0569
DOPPEL SPIDER
DragonOK
Earth Estries
Earth Kitsune
ENERGETIC BEAR
FIN6
FIN7
Flax Typhoon
Flying Kitten
Fox Kitten
Frankenstein
Fxmsp
Gangnam Industrial Style
GOLD DUPONT
GOLD GALLEON
GOLD SKYLINE
Grayling
Hagga
Inception Framework
Infy
Karakurt
LAPSUS
Lucky Cat
Madi
MosesStaff
Unknown
China
Vietnam
Iran
North Korea
Colombia
Russia
India
Lebanon
Ukraine

Threat Landscape

KNOW THY ENEMY, KNOW THYSELF

97

Advanced Persistent Threats (APTs)

1,482

Tactics, techniques & procedures

1,708

Aanvalstools

ONS BEELD VAN JOUW OMGEVING

Hoe?

Wachtwoorden

Phishing

Missende Patches

BINNEN

Blocked, Opnieuw

'Vergeten' alerts

Wachtwoorden

Missende Patches

Configuratie

DOOR

Geen zichtbaarheid

Response onduidelijk

Informatie diefstal

Ransomware

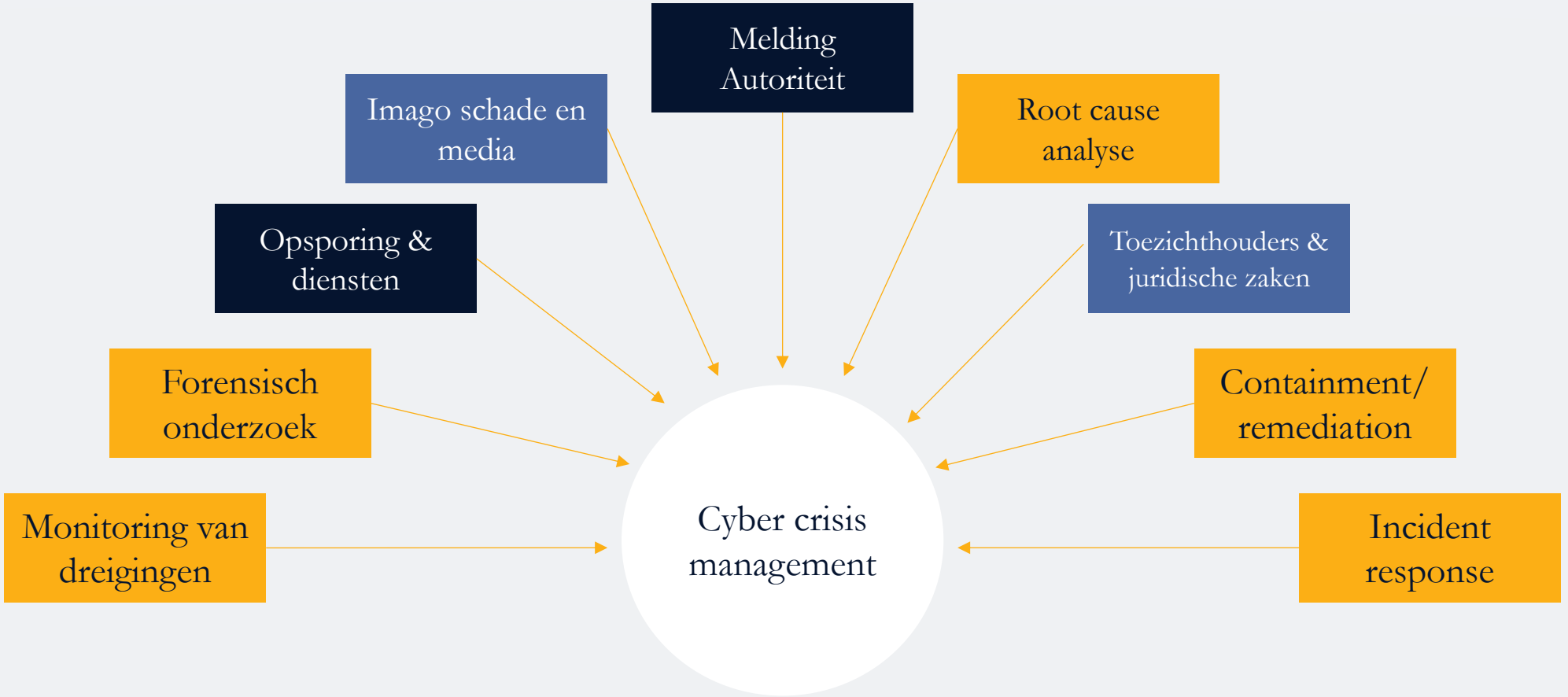
UIT

Geen logs

Geen retentie

IR Crisis management

DE COMPLEXITEIT VAN VERSCHILLENDE DILEMMA'S & BELANGHEBBENDEN



PRIORITEITEN

Initiële Triage

- Scherp krijgen wat nu eigenlijk de situatie is, bepaal de:
  - Scope, en;
  - (Mogelijke) Impact.
- Eerste 48 uur staan in het teken van begrip verkrijgen van wat de situatie is. Is het serieus, een *false-positive*, beperkte scope of wijdverbreid?
- Dus, waar staan we nu, en wat weten we zeker, wat weten we zeker niet, en wat zijn eventuele onzekerheden.

PRIORITEITEN

Crisismanagement & Communicatie

- In kaart brengen risico's
  - Welke data is getroffen?
  - Welke (criminele) scenario's zijn denkbaar?
- Communicatie medewerkers, klanten, en media
  - Intern bericht
  - Extern bericht
- Juridisch | Verzekering | Aansprakelijkheid
- Opsporing/aangifte politie

PRIORITEITEN

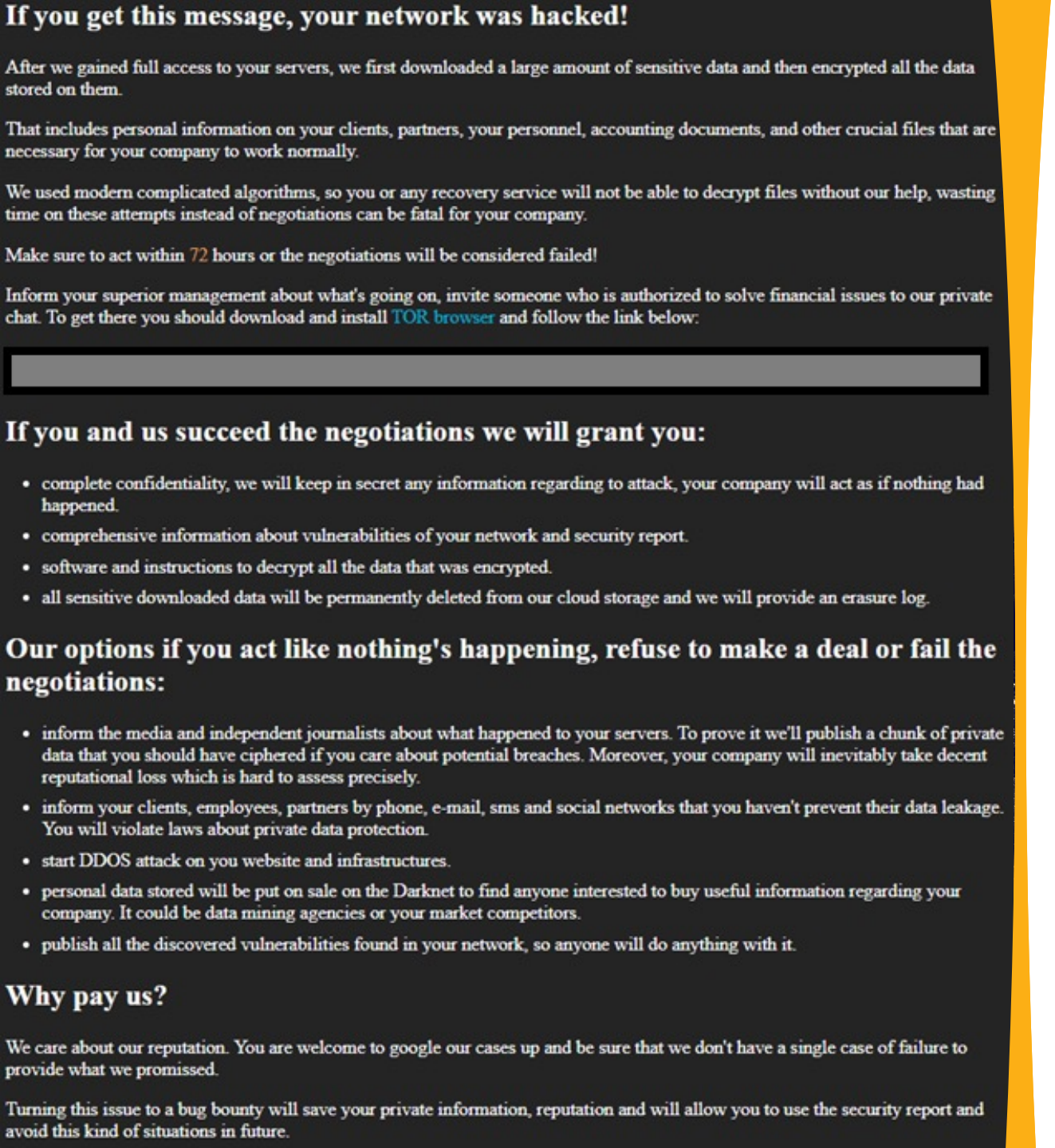
Business Continuïteit

- Beschikbaarheid systemen: back-ups terugzetten en veilig stellen ten einde dienstverlening z.s.m. weer operationeel te krijgen;
- Hardening van systemen:
  - Op basis van IOCs;
  - Monitoring netwerk;
  - Aanvullende beveiligingsmaatregelen;
- De (bedrijfs) impact van de aanval minimaliseren;
- Back-up- en herstelstrategieën te coördineren en te ondersteunen bij de uitvoering;

PRIORITEITEN

Root Cause Analyse

- Het veiligstellen en onderzoeken van digitaal forensisch bewijsmateriaal;
- Onmiddellijk inzicht te verkrijgen in dreiging door middel van eerste triage;
- Grondig forensisch onderzoek uit te voeren naar de oorzaak van de inbreuk;
- Bevindingen van het onderzoek dag/wekelijks rapporteren;
- Op basis van de bevindingen uit het onderzoek systemen beter beveiligen in het belang van business continuïteit.



If you get this message, your network was hacked!

After we gained full access to your servers, we first downloaded a large amount of sensitive data and then encrypted all the data stored on them.

That includes personal information on your clients, partners, your personnel, accounting documents, and other crucial files that are necessary for your company to work normally.

We used modern complicated algorithms, so you or any recovery service will not be able to decrypt files without our help, wasting time on these attempts instead of negotiations can be fatal for your company.

Make sure to act within 72 hours or the negotiations will be considered failed!

Inform your superior management about what's going on, invite someone who is authorized to solve financial issues to our private chat. To get there you should download and install TOR browser and follow the link below:

If you and us succeed the negotiations we will grant you:

- complete confidentiality, we will keep in secret any information regarding to attack, your company will act as if nothing had happened.
- comprehensive information about vulnerabilities of your network and security report.
- software and instructions to decrypt all the data that was encrypted.
- all sensitive downloaded data will be permanently deleted from our cloud storage and we will provide an erasure log.

Our options if you act like nothing's happening, refuse to make a deal or fail the negotiations:

- inform the media and independent journalists about what happened to your servers. To prove it we'll publish a chunk of private data that you should have ciphered if you care about potential breaches. Moreover, your company will inevitably take decent reputational loss which is hard to assess precisely.
- inform your clients, employees, partners by phone, e-mail, sms and social networks that you haven't prevent their data leakage. You will violate laws about private data protection.
- start DDOS attack on you website and infrastructures.
- personal data stored will be put on sale on the Darknet to find anyone interested to buy useful information regarding your company. It could be data mining agencies or your market competitors.
- publish all the discovered vulnerabilities found in your network, so anyone will do anything with it.

Why pay us?

We care about our reputation. You are welcome to google our cases up and be sure that we don't have a single case of failure to provide what we promissed.

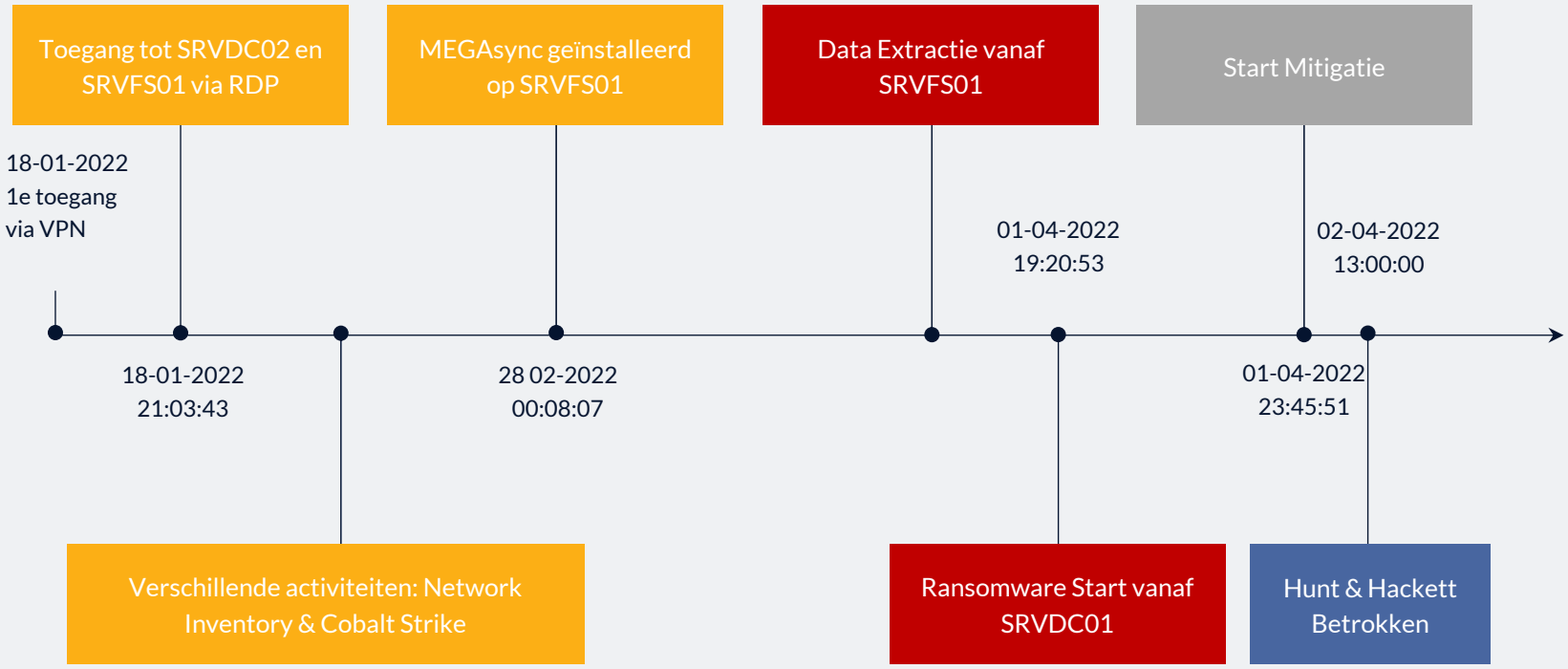
Turning this issue to a bug bounty will save your private information, reputation and will allow you to use the security report and avoid this kind of situations in future.

Praktijk Voorbeeld

ROOT CAUSE ANALYSE BIJ
DRIEVOUDIGE AFPERSING

Tijdlijn van het incident

HOOG OVER WEERGAVE VAN SLEUTEL MOMENTEN IN DE AANVAL



- [Eerste activiteit] aanvaller geobserveerd op 18 januari 2022
- [Account misbruik] VPN, Administrator en Active Directory
- [Aanvalstools] MEGAsync, TNI, PCHunter en Cobalt Strike
- [Toegang Russisch IP] op 01 April 2022 om 21:11:39 met persoonlijk VPN account

Hoofdbevindingen

OP BASIS VAN HET AANGELEVERDE SYSTEMEN EN OVERIGE LOGGING

- [Initiële toegang] door middel van VPN account service leverancier zonder multi-factor authenticatie (MFA)
- [Laterale bewegingen] door het netwerk met intern administrator account
- [Bur3n@dm1n$!] wachtwoord lijkt sterk, maar is dit niet
- [Malafide software] uitvoer en installatie onopgemerkt gebleven, of niet gereageerd op antivirus meldingen
- [Data extractie] heeft plaatsgevonden vanaf de bestandserver

Detectie matrix

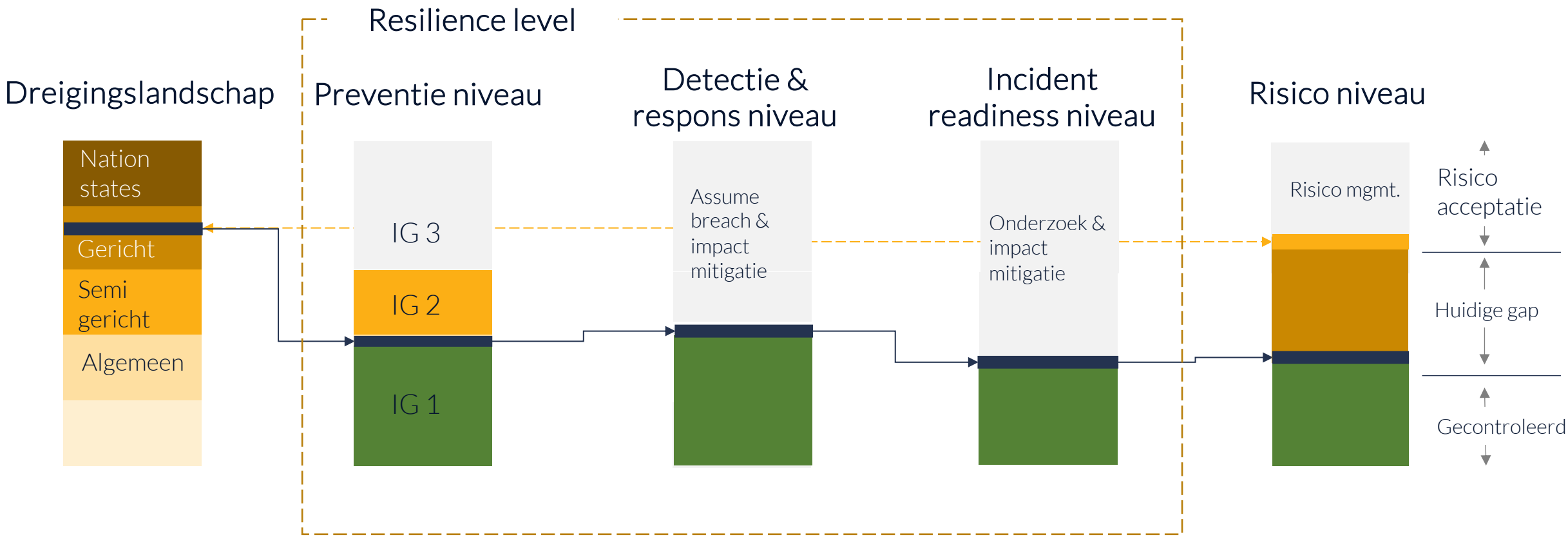
FASEN VAN DE AANVAL WAARIN DETECTIE MOGELIJK WAS

Gebruikte technieken:

1. Login van ongebruikelijke locatie
2. Login van blocklist locaties (bijv. Rusland, China).
3. RDP login van ongebruikelijke locatie (buiten allowlist)
4. Detectie van offensieve tool Cobalt Strike op endpoints
5. Network gebaseerde login van het administrator account
6. Wijziging van groepen met verhoogde rechten
7. Installatie en uitvoer van bekend dubieuze software (TNI, PCHunter, MEGAsync, Cobalt Strike, etc.)
8. Detectie van verschillende technieken om accountinformatie te bemachtigen
9. Grote afwijkingen in verkeersstromen
10. Uitzetten van services die verwant zijn aan back ups van data
11. Detectie van proces dat verdachte (encryptie) activiteit uitvoert

Preventie | Detectie | Response

WAT IS JOUW CYBERSECURITY RISICO BLOOTSTELLING GEZIEN VANUIT HET DREIGINGSLANDSCHAP



Managed Detection & Response

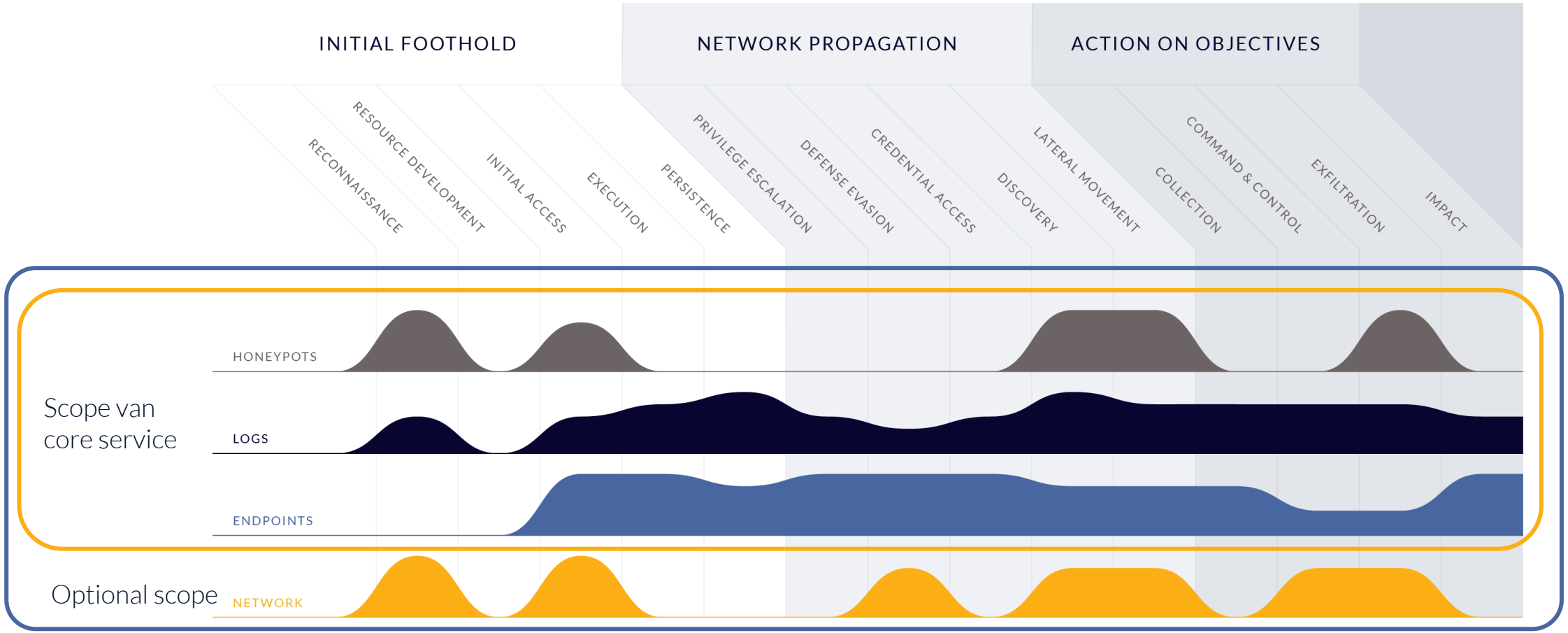
MANAGED DETECTION & RESPONSE

Wat is MDR?

- Monitoring en analyse van security alerts door ervaren analisten
- Het doel is vroegtijdige detectie van incidenten, zodat verdere escalatie naar een serieus incident voorkomen kan worden
- Analisten kunnen reageren op alerts, door interactief op systemen in te grijpen, binnen de kaders van het response mandaat

Zichtbaarheid over de aanvalsketen

DATA BRON ZICHTBAARHEID MET LOGS, ENDPOINT & HONEYPOT MONITORING



KEY COMPONENTS OVERVIEW

Cybersecurity Resilience Framework

INTERACTIEVE WORKSHOP

Responding to ransomware

Wij organiseren regelmatig roundtable sessies en workshops bij ons op kantoor. In deze sessies brengen we directieleden en technische experts samen voor interessante discussies over cyber security.

De volgende sessie vindt plaats op **20 juni van 15:30 tot 18:00** bij ons op kantoor in **Den Haag.**

We nodigen je graag uit voor deze **interactieve workshop** waarin je een geanonimiseerd ransomware-scenario doorloopt. Tijdens deze workshop ervaar je de typische fases van een digitale (ransomware) aanval en kun je je praktisch voorbereiden op een mogelijke aanval.

Aanmelden kan via:
https://www.huntandhackett.com/cyberconnect

Kun je niet aanwezig zijn bij deze sessie, maar wil je op de hoogte blijven van toekomstige sessies? Meld je aan voor onze nieuwsbrief via: https://www.huntandhackett.com/keep-me-informed

/whoami

Mattijs Dijkstra

dijkstra@huntandhackett.com

+31 6 107 367 22

+31 70 222 00 00

Anna van Buerenplein 46

2595 DA - Den Haag