Cyber Threat Intelligence

Matthijs van Polen

OVER MIJ

MATTHIJS VAN POLEN

NU:
SOC OPS, CTI @ Northwave

HIERVOOR:

Solutions Architect @ EclecticIQ (via Northwave)

Implementatiebegeleider @ Quarantainenet

CTI ONTLEED

Cyber

cy·ber-
(in samenstellingen) in cyberspace bestaand, op internet; = virtueel: *cyberaanval*, *cybercafé*, *cybergeld*, *cyberstore*, *cyberwereld*

Threat

dreiging

dat wat gevaar oplevert

Intelligence

inlichtingen

dus niet: intelligentie

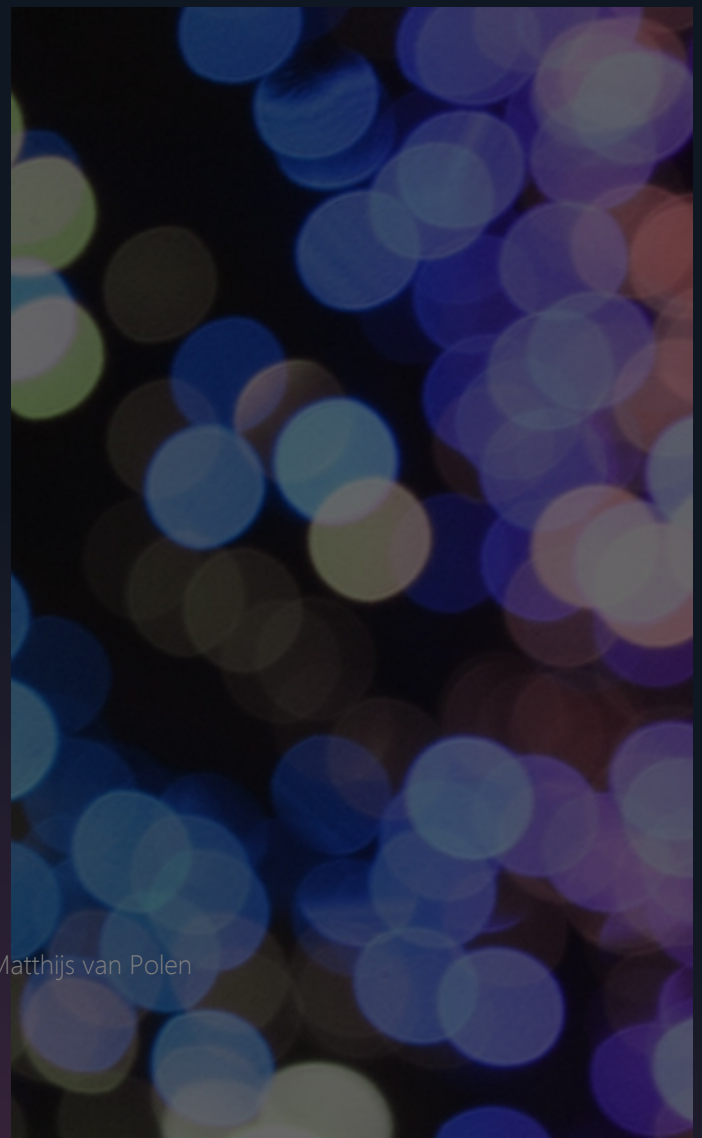
INLICHTINGEN

- Veel verschillende definities
- Overeenkomst:

  Informatie die helpt bij het maken van beslissingen.

WAAROM CTI?


70



PROBLEEM

HET KLASSIEKE VERDEDIGINGSMODEL IS REACTIEF

- Loopt achter de feiten aan

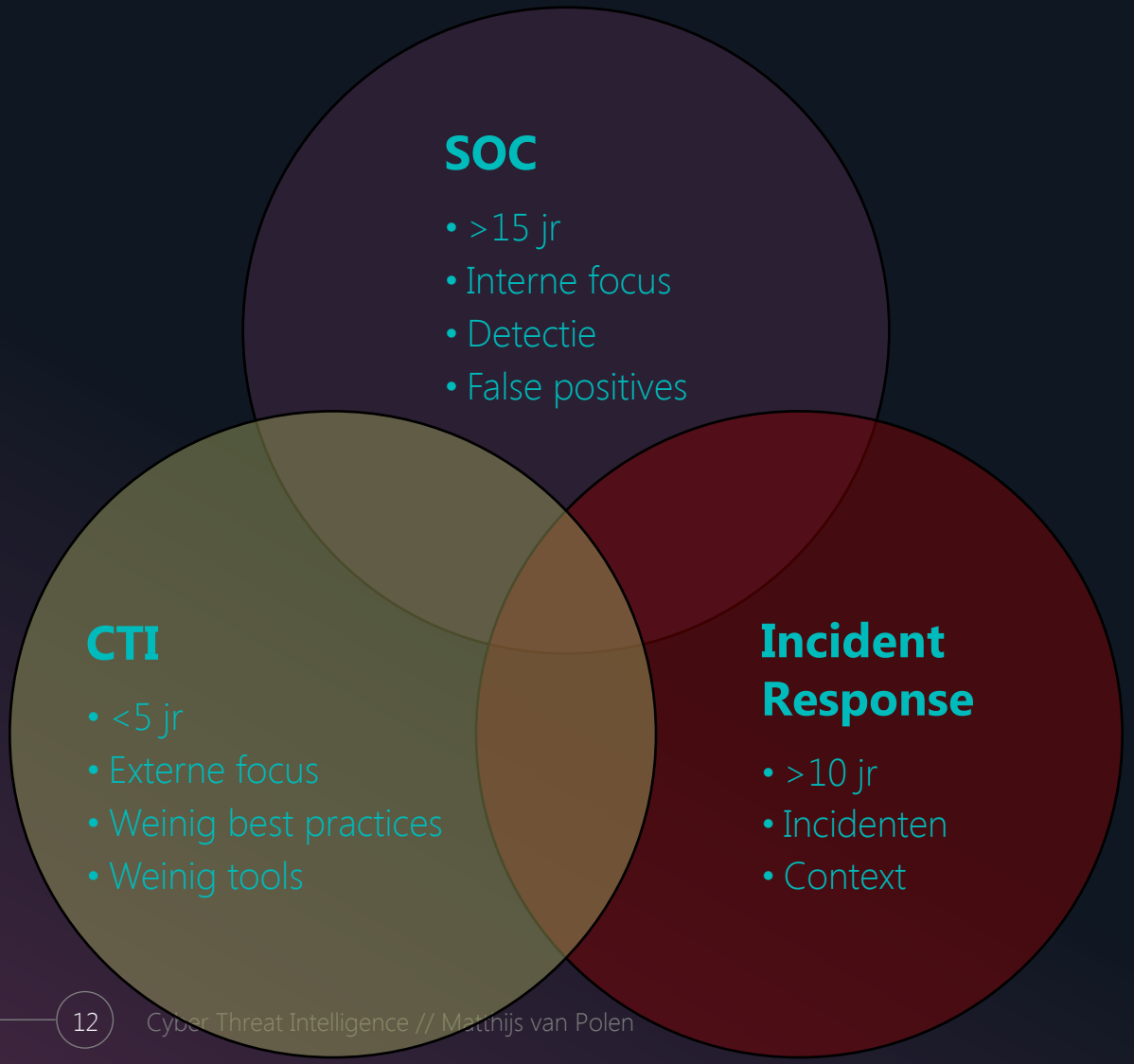
OPLOSSING

- Vooruit kijken
- Naar buiten kijken
- Wat gaat er op me af komen?

- Kortom: CTI!

Wie maakt er al gebruik van CTI?

CTI en andere practices



NIVEAUS

Strategisch

- Wie is die tegenstander uberhaupt?
- Waar zijn we zoal bezorgd om?
- Risk management, compliancy, policy management

Operationeel

- Het strategische naar het tactische vertalen
- Wat voor capabilities hebben we nodig?
- Security operations, vulnerability management, fraude

Tactisch

- Wat is er **nu** nodig om de vijand aan te pakken?
- IOCs
  - File-hashes
  - C2-servers
  - Etcetera
- Incident operations, incident response

HOE GAAT DAT DAN?

STAKEHOLDERS

VOOR WIE DOEN WE HET EIGENLIJK

BUSINESS

Uitbreiding naar het buitenland.
China? Rusland? Afrika?

BRAND

Misbruikt iemand onze naam?

SOC/IR

Context bij incidentresponse

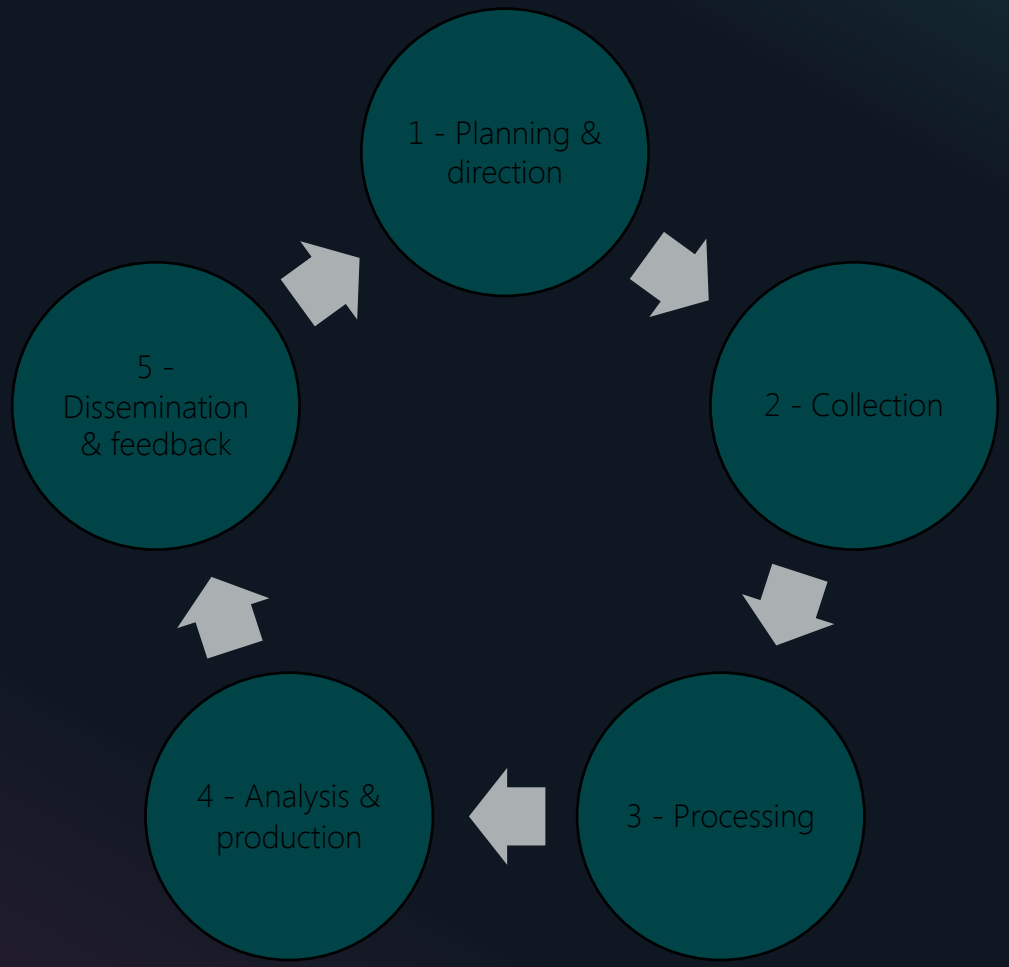
Juiste IOCs om op te alarmeren

FRAUDE

Money mules

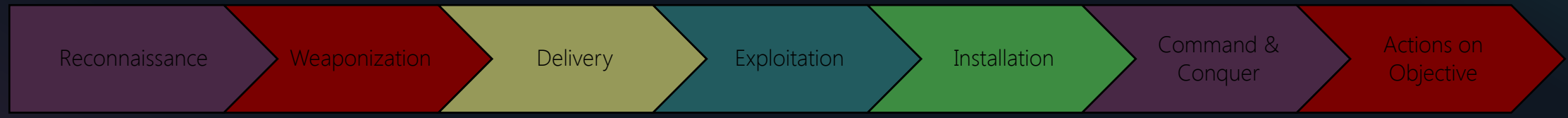
Creditcardfraude

INTELLIGENCE CYCLE



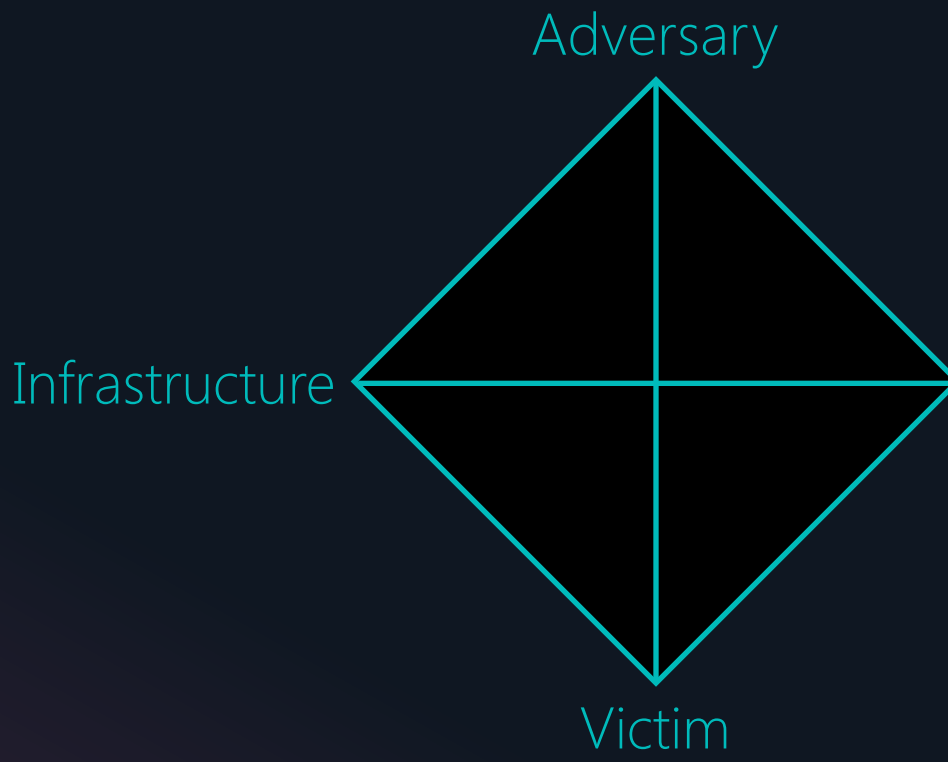
Wie is er bekend met de Cyber Kill Chain?

CYBER KILL CHAIN



Wie is er bekend met het Diamond Model?

DIAMOND MODEL



DIAMOND MODEL

FUZZYSQUIRREL

Specifieke Chinese Universiteits-IP-adressen

Poison Ivy met specifieke mutex

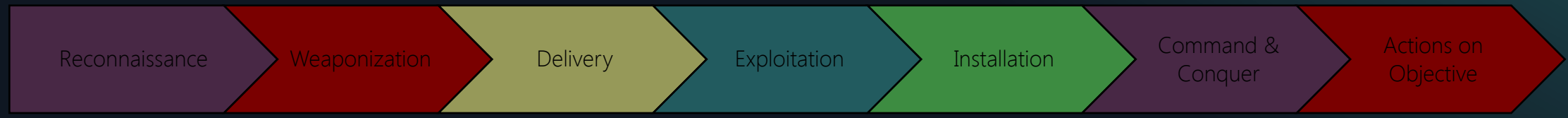
Chinese Dissidenten

ANGRYHIPPO

Google Docs & specifieke Chinese Universiteits-IP-adressen

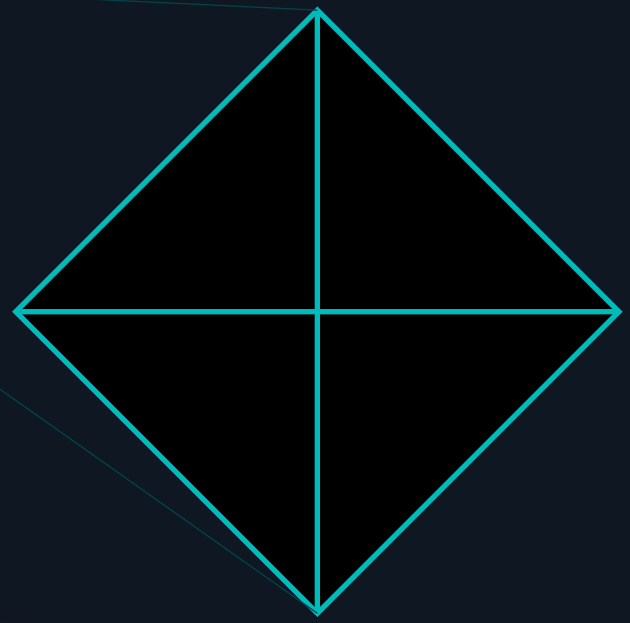
Taiwanese democratische kandidaten

Cyber Kill Chain & Diamond Model



John Doe @ Evil Corp

Outlook Express
john.doe@outlook.com



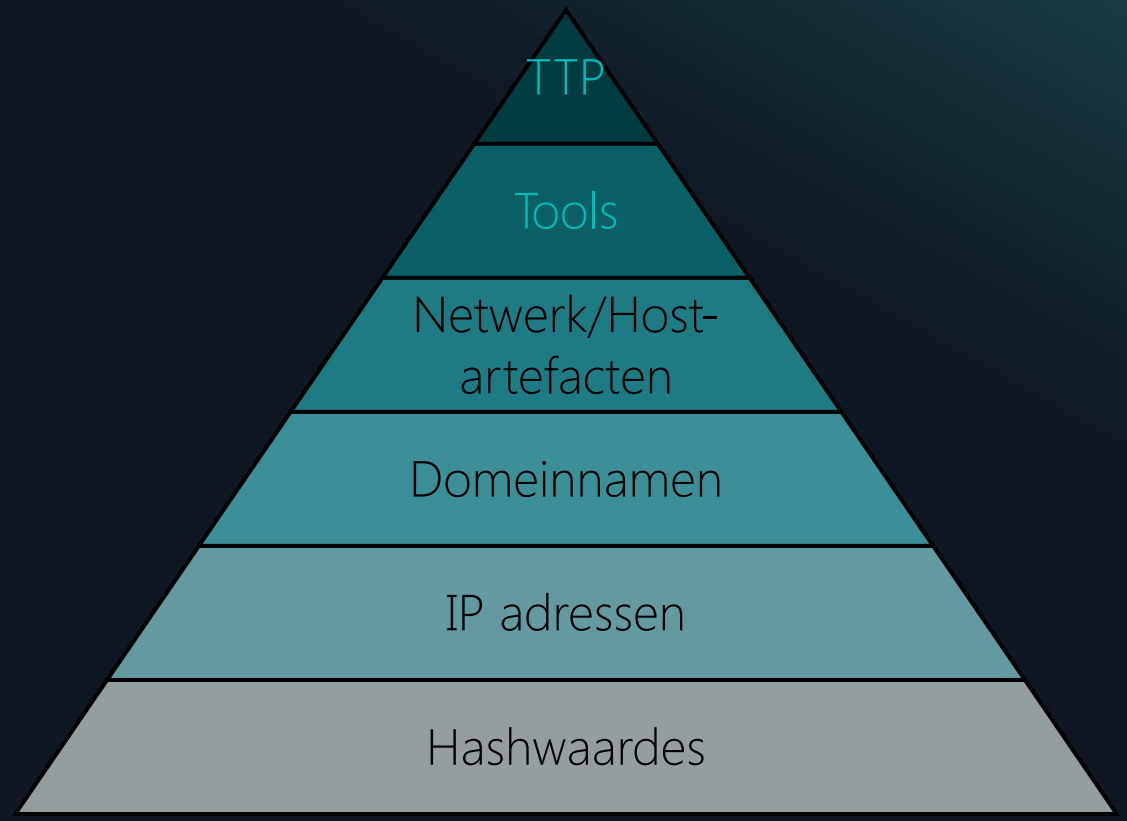
Phishing email
PDF met malware

Floris van Financiën

PYRAMID OF PAIN

- Hashes van bestanden zijn triviaal te veranderen
- IP adressen: erg eenvoudig
- Domeinnamen: simpel
- Netwerk/host-artefacten: vervelend
- Tools: lastig
- TTPs: moeilijk!

  TTP: Tactics, techniques, procedures



MITRE ATT&CK

Spearphishing Link

Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging User Execution. The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons). Links may also direct users to malicious applications designed to Steal Application Access Tokens, like OAuth tokens, in order to gain access to protected applications and information.[1]

ID:
Ta
Pl
Da
ga
re
CA
Co
We
Pl
Mi
Ve

Procedure Examples

Name	Description
APT28	APT28 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redi

OMDRAAIEN

- Intel gaat omhoog
  - Intrusie
  - Campagne
  - Natie-staat
- Besluiten gaan omlaag
  - Businessbeslissingen
  - Collectie, verwerken, capabilities
  - Alerts

OBJECTIVITEIT

- Schakel je gevoel uit, kijk objectief. Gebruik “estimative language”
- Structured Analytic Techniques
  - Analysis of Competing Hypotheses (ACH)

Will Competitor X bid on an upcoming contract?	*H1: Yes - as a prime*	*H2: Yes - as a subcontractor*	*H3: No - they will not bid*
E1: Competitor X has relevant past performance	C	C	I
E2: Customer is looking for strong cybersecurity capabilities	C	C	I
E3: Competitor X's business development lead for this customer recently left	I	C	C
E4:...			
E5:...			

VERPAKKING

Strategisch

- Rapport
- Dreigingsbeeld

Operationeel

- Iets specifieker, meer gericht op specifieke capabilities.
- Memo

Tactisch

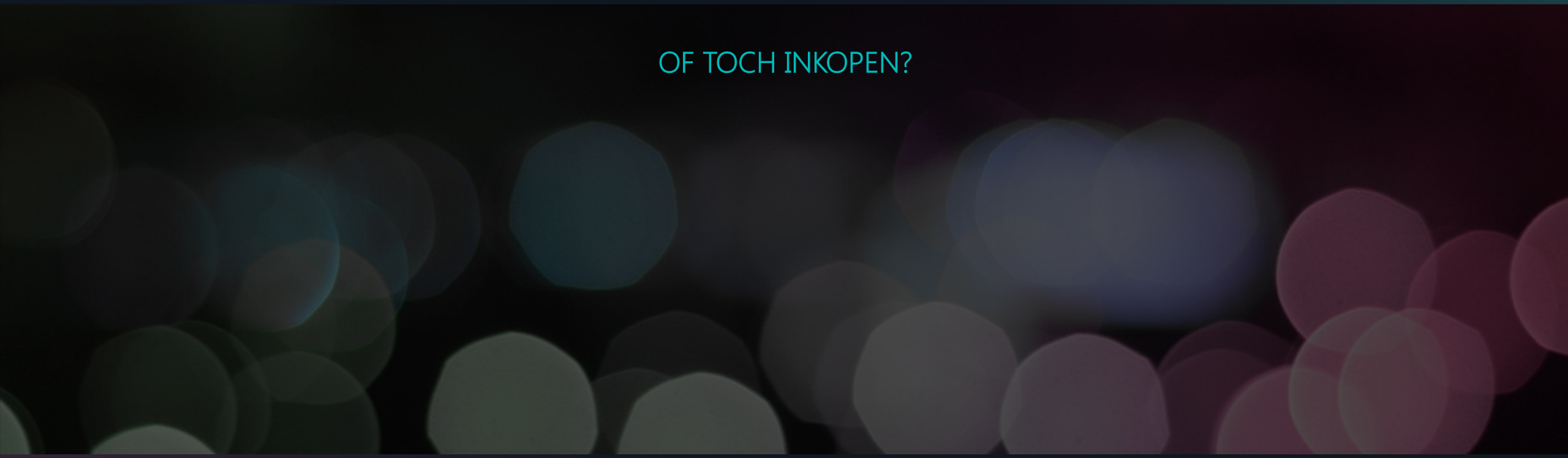
- IOCs
  - File-hashes
  - C2-servers
  - Etcetera
- Feed, CSV, voor bv. SIEM

TIPJE VAN DE IJSBERG

HEEL VEEL MEER OVER HET WERKVELD

- SANS FOR578
- Intelligence Analysis: A Target-Centric Approach - Robert M. Clark
- Psychology of Intelligence Analysis – Richards Heuer

ZELF DOEN?



OF TOCH INKOPEN?

STAKEHOLDERS

VOOR WIE DOEN WE HET EIGENLIJK

BUSINESS

Uitbreiding naar het buitenland.
China? Rusland? Afrika?

BRAND

Misbruikt iemand onze naam?

SOC/IR

Context bij incidentresponse

Juiste IOCs om op te alarmeren

FRAUDE

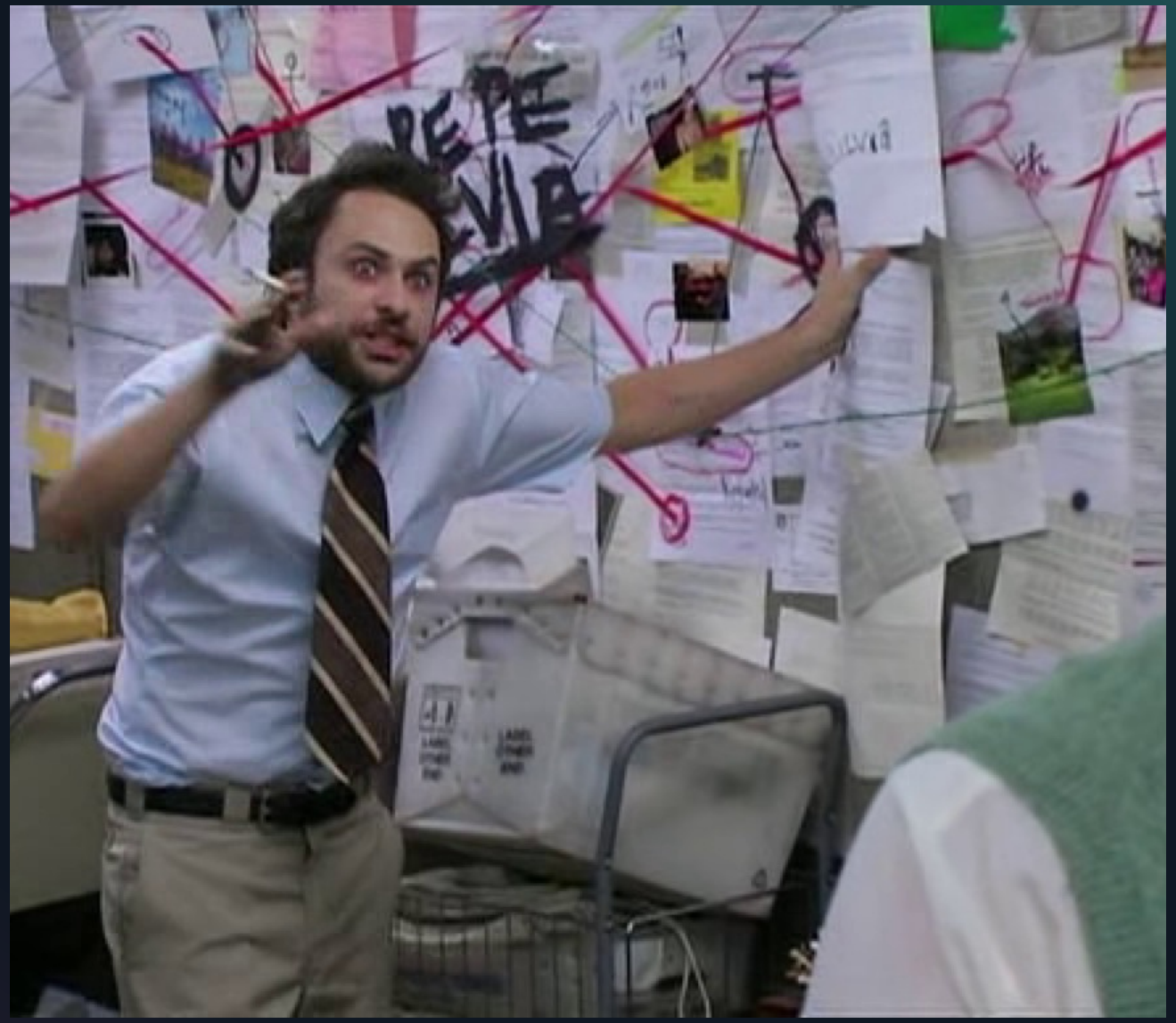
Money mules

Creditcardfraude

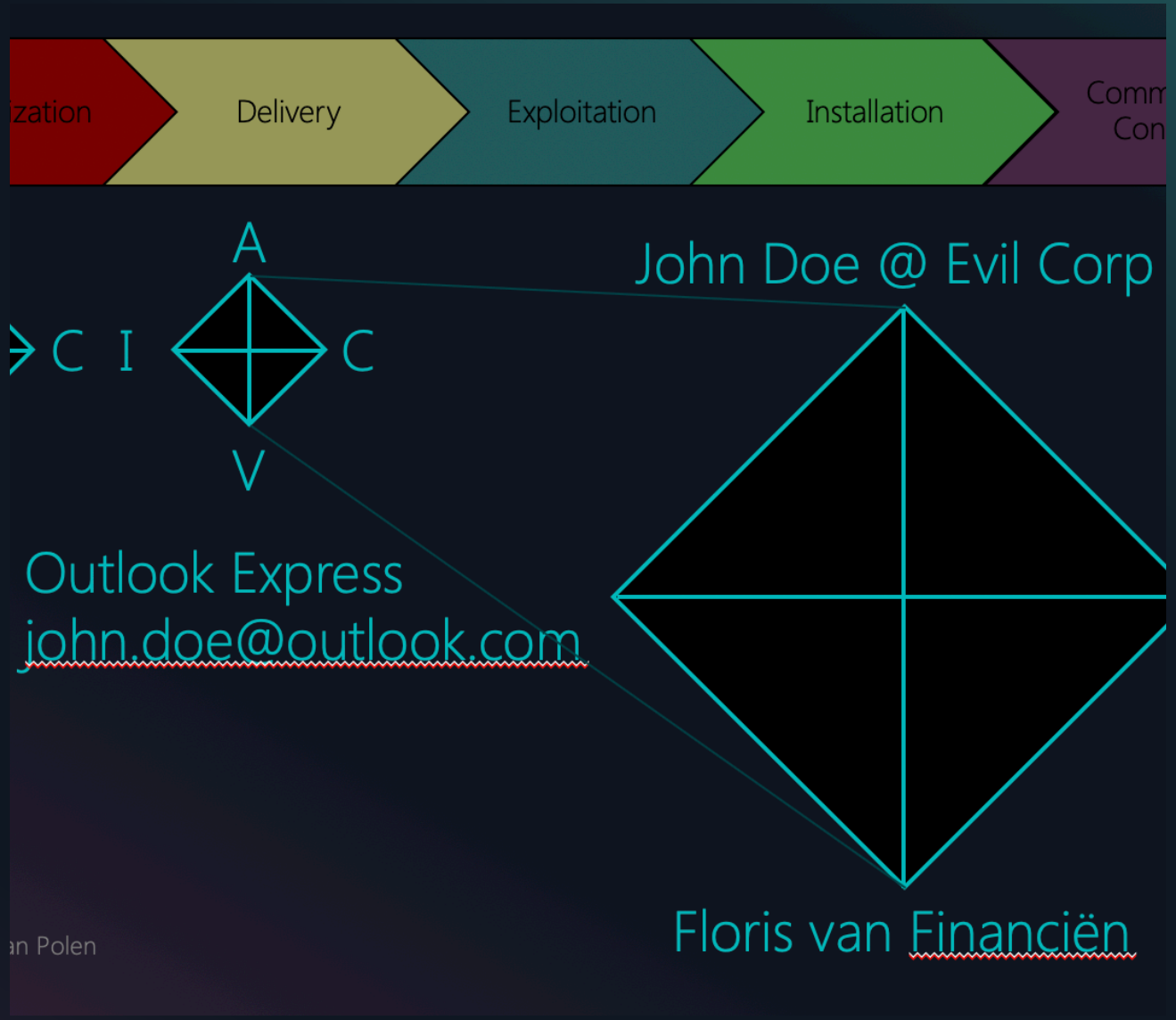
Zelf doen

Wie heeft er een eigen CTI team?

Je kent je eigen organisatie het best



Waardevolle data in eigen intrusies



SPECIFIEK WERK

- Overlap met SOC, IR, maar wel duidelijk andere vaardigheden.
- Non-cyberervaring heel nuttig
  - Politiemedewerkers
  - Landenkenners

HULP BIJ ZELF DOEN

- Ga niet zelf web scrapen
- Koop data en tools die helpen met ontginnen van data
  - Intel 471
  - Silobreaker

- Vrij stevig werk. Grote organisaties! Shell, ING, Rabobank

INKOPEN

Wie wil er een eigen CTI team?

Terug naar niveaus

- Strategisch
- Operationeel
- Tactisch

	Consumers	Effects	Product
Strategic	Executives, BAISOs	Business strategy risk calculus	Nation-state **Threat Assessments**
Operational	CIS, CIRT, customers, some peers	Investment priorities, capabilities, comprehensive intel, data access	**Campaign analysis**
Tactical	CIRT, partners	Mitigations, detections, “IR”	**KC completion**

Strategische intel

- Het gaat altijd over context
- Hoog-over berichten zijn te koop
- Maar ook gratis te vinden

Operationeel

- Informatie over campaigns
- Te koop, ook open source
- Bruikbaar voor SOC, IR
- Vaak hand-in-hand met tactische inlichtingen

Tactisch

- IOCs
- Voor SIEM, IDS, Firewall
- Vaak inbegrepen bij betreffende producten
- Vaak hand-in-hand met operationele inlichtingen
- Genoeg open source te vinden

EN NU?

ZELF DOEN

- Goed overleg met stakeholders
- Eigen organisatiekennis
- Kost tijd, kost veel geld
- Requirements goed stellen

INKOPEN

- Goed overleg met stakeholders
- Kost soms ook veel geld
- Indicatorfeeds goed aan te komen
  - Relevantie soms een issue
- Snel bruikbaar.
- Requirements goed stellen

BRONNEN

- https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492183308.pdf
- Intelligence Analysis: A Target-Centric Approach – Robert M. Clark
- Psychology of Intelligence Analysis – Richards Heuer

BEDANKT!

Matthijs van Polen

Phone:
+31 6 28 24 72 31

Email:
matthijs.v.polen@northwave.nl

LinkedIn:
www.linkedin.com/in/matthijsvanpolen