Christian Dinesen

Combitech

Dansk IT

MEET & INSPIRE
THREAT INTELLIGENCE - HVORDAN OG HVORFOR?

4. FEBRUAR 2020
Christian Dinesen

AGENDA

- Hvorfor man bør kigge på Threat Intelligence
- Hvad Threat Intelligence ikke er
- Hvordan man kommer i gang med Threat Intelligence
- Afsluttende dialog

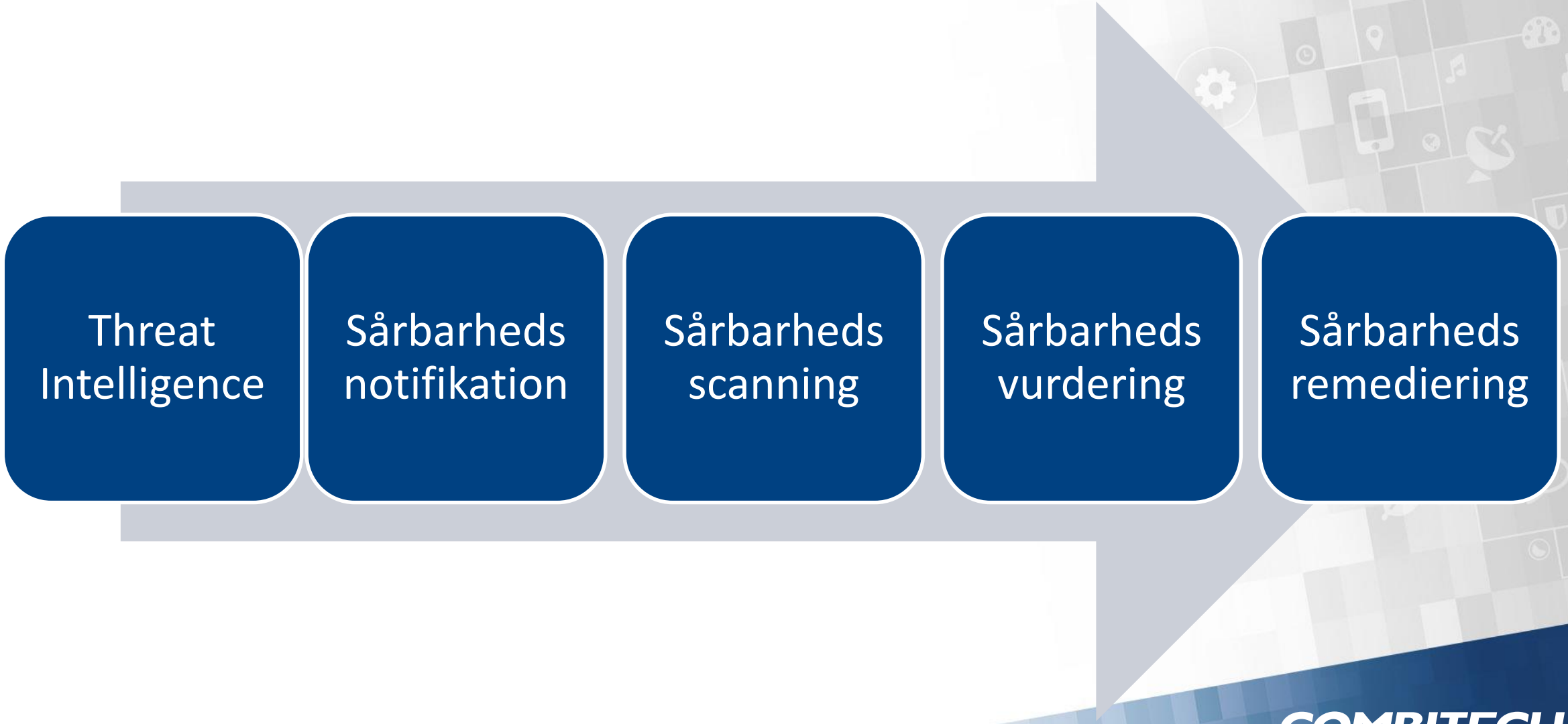
COMBITECH

HVORFOR MAN BØR KIGGE PÅ THREAT INTELLIGENCE

- Håndtere de generelle trusler, der kan ramme alle
- Kunne informere ledelsen på oplyst grundlag
- Behandler specifikke trusler, der ligger uden for virksomhedens infrastruktur
- Kunne være up-to-date med hensyn til de nyeste angrebsmetoder, mål og angribere
- Analysere ekstern data om trusler eller data læk
- Etablering af et bedre forsvar for proaktivt at reagere på trusler og bruge det til at analysere angrebsfladen

COMBITECH

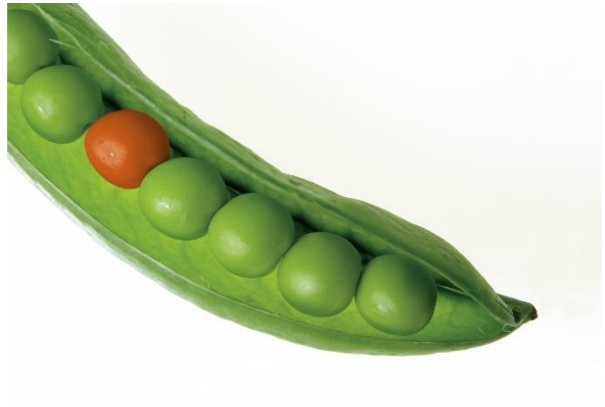
EKSEMPEL PÅ FLOW



COMBITECH

HVORFOR ER THREAT INTELLIGENCE ANDERLEDES

- Det er en anden type medarbejdere, kompetencer og personprofiler end normal security
- Man skal kunne arbejde meget med risiko og tage ”svære” beslutninger



- Der skal dagligt monitoreres flere hundrede data sources, enten systematisk eller fra løsning
- Datalæk sker kontinuerligt og der skal overvåges efter fx password
- Offentlige eksponerede services risikerer trusler for udnyttelse
- Skal have en bedre viden om de trusler som reelt kan påvirke forretningen og holde relevante stakeholdere informeret om de nyeste trusler og de konsekvenser de kan have

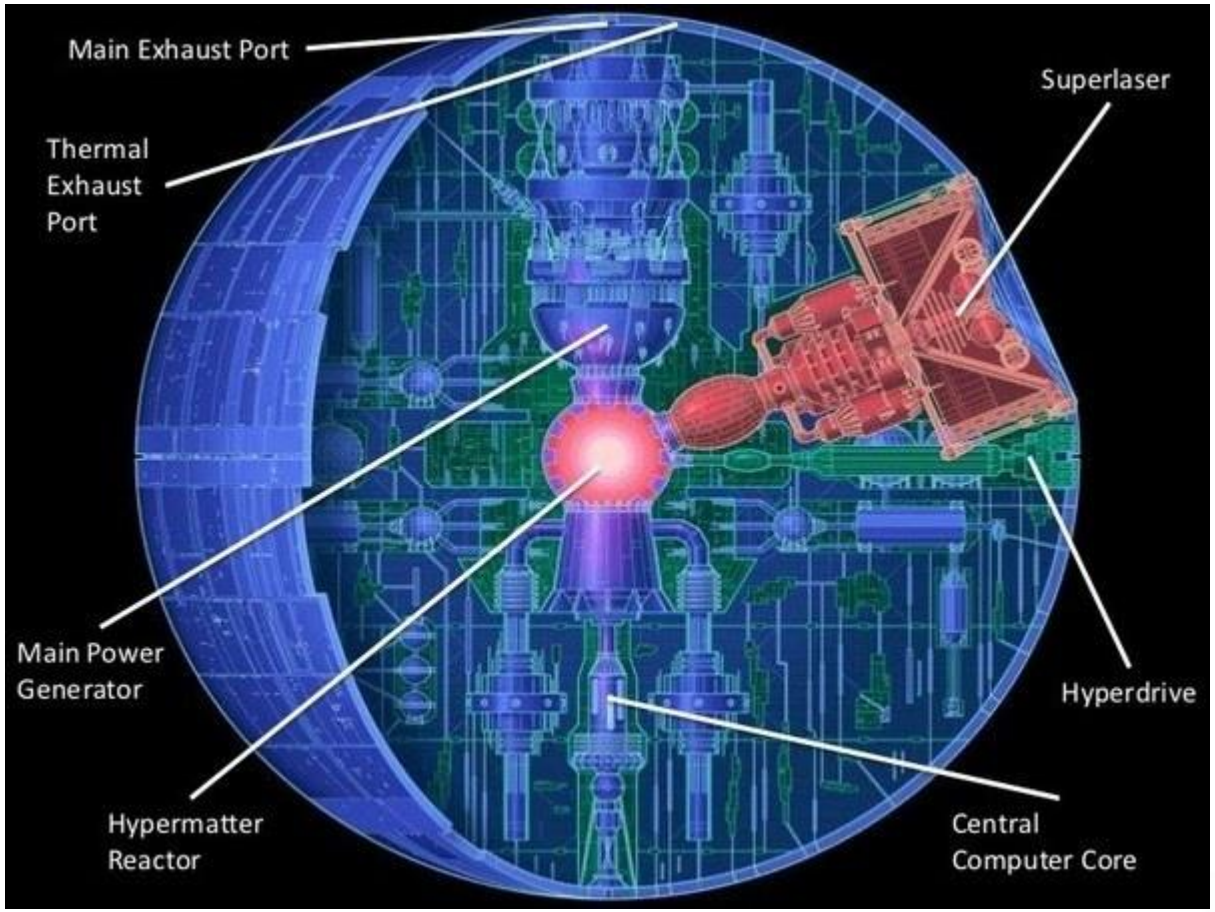
COMBITECH

KONTINUERLIGT ELLER AD HOC

- Skal det leveres som en service, en mail eller ad hoc?
- Skal der være fokus på det generelle ($)
- Skal der være fokus på det specifikke ($$)
- Skal der laves kontinuerlig trussels indsamling ($$$)

HVEM ER THREAT INTELLIGENCE FOR?

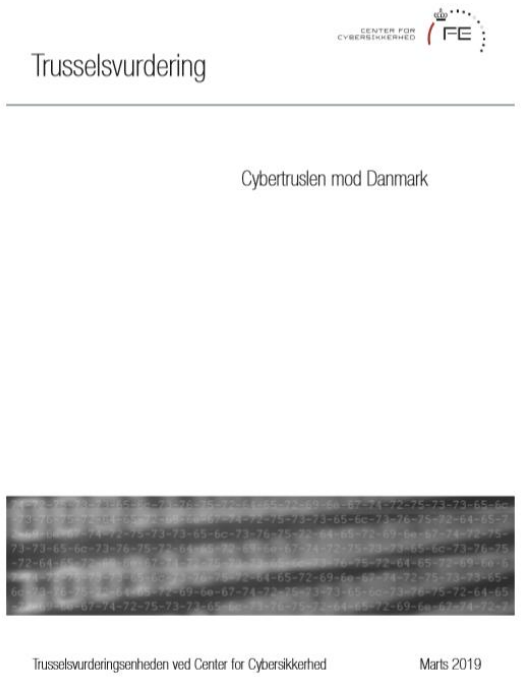
- Det er ikke kun for forsvarsindustri, pengeinstitutter og andre med eksotiske fjendtlige aktører
  - Det er også relevant for os personligt
- Skulle dødsstjernens port være beskyttet bedre?



COMBITECH

HVAD THREAT INTELLIGENCE IKKE ER

- Sårbarhedsnotifikationer
- Vulnerability scanning
- Nationale trusselsvurderinger



Recorded Future

Microsoft Targeted by 8 of 10 Top Vulnerabilities in 2018

Cyber Vulnerability	References	Company
CVE-2018-8174	567	Microsoft
CVE-2018-4878	387	Adobe
CVE-2017-11882	223	Microsoft
CVE-2017-8750	192	Microsoft
CVE-2017-0199	91	Microsoft
CVE-2016-0189	78	Microsoft
CVE-2017-8570	68	Microsoft
CVE-2018-8373	66	Microsoft
CVE-2012-0158	55	Microsoft
CVE-2015-1895	49	Google Android

COMBITECH

EKSEMPLER PÅ LEVERANDØRER

FIREEYE™

kaspersky

Recorded Future

COMBITECH

OPEN SOURCE DER KAN HJÆLPE TIL

MISP
Threat Sharing

CISA
CYBER+INFRASTRUCTURE
Search
REPORT
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
Cybersecurity > Information Sharing > Automated Indicator Sharing (AIS)
Information Sharing
Automated Indicator Sharing (AIS)
AUTOMATED INDICATOR SHARING (AIS)
The Department of Homeland Security's (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange
en the Federal Government and the private sector at machine speed. Threat indicators
alicious IP addresses or the sender address of a phishing email (although they can also

Threat Level:
Internet Storm Center
Keyword, Domain, Port, IP or Hea
Search
Participate: Learn more about our honeypot network
https://isc.sans.edu/honeypot.html
Contact Us
Diary
Podcasts
Jobs
Tools
Data
Forums
Questions? Feedback?
Use our contact form or
report bugs here
Last Daily Podcast (Mon, Feb 3rd): Stego & Cryptominers; Cornavirus Scams; Google OpenSK
Latest Diaries
Analysis of a triple-encrypted AZORult downloader
Published: 2020-02-03
Last Updated: 2020-02-03 07:07:13 UTC
by Jan Kopriva (Version: 1)
0 comment(s)
I recently came across an interesting malicious document. Distributed as an attachment of a run-of-the-mill malspam message, the file with a DOC extension didn't look like anything special at first glance. However, although it does use macros as one might expect, in the end, it turned out not to be the usual simple maldoc as the following chart indicates.

cisco Talos

SPAMHAUS
THE SPAMHAUS PROJECT
SBL | XBL | PBL | DBL | DROP | ROKSO
Blocklist Removal Center
About Spamhaus | Contacts | Official Statements | Sponsors | FAQs | News Blog

HVORDAN MAN KOMMER I GANG MED THREAT INTELLIGENCE

- Lær af de industrier hvor det har været brugt gennem mange år
  - Map til relevante risici i virksomheden
- Kik på forskellige Threat feeds
  - Både open source og kommercielle
- Få demo i en længere periode fra forskellige leverandører
- Vurdér de nationale Trusselsvurderinger
- Map til MITRE
- Er du/I klar?
  - Hvordan håndterer vi en notifikation om en trussel
  - Hvem kigger vi på og hvem sammenligner vi os med
  - Hvordan er vores beredskab, hvor hurtigt kan vi reagerer 24/7
  - Er rollerne fordelt og kender vi dem som skal have informationerne
  - Kender vi vores prioriteter og har vi en kill switch
  - Hvad har vores medarbejdere af information

ATT&CK™

COMBITECH