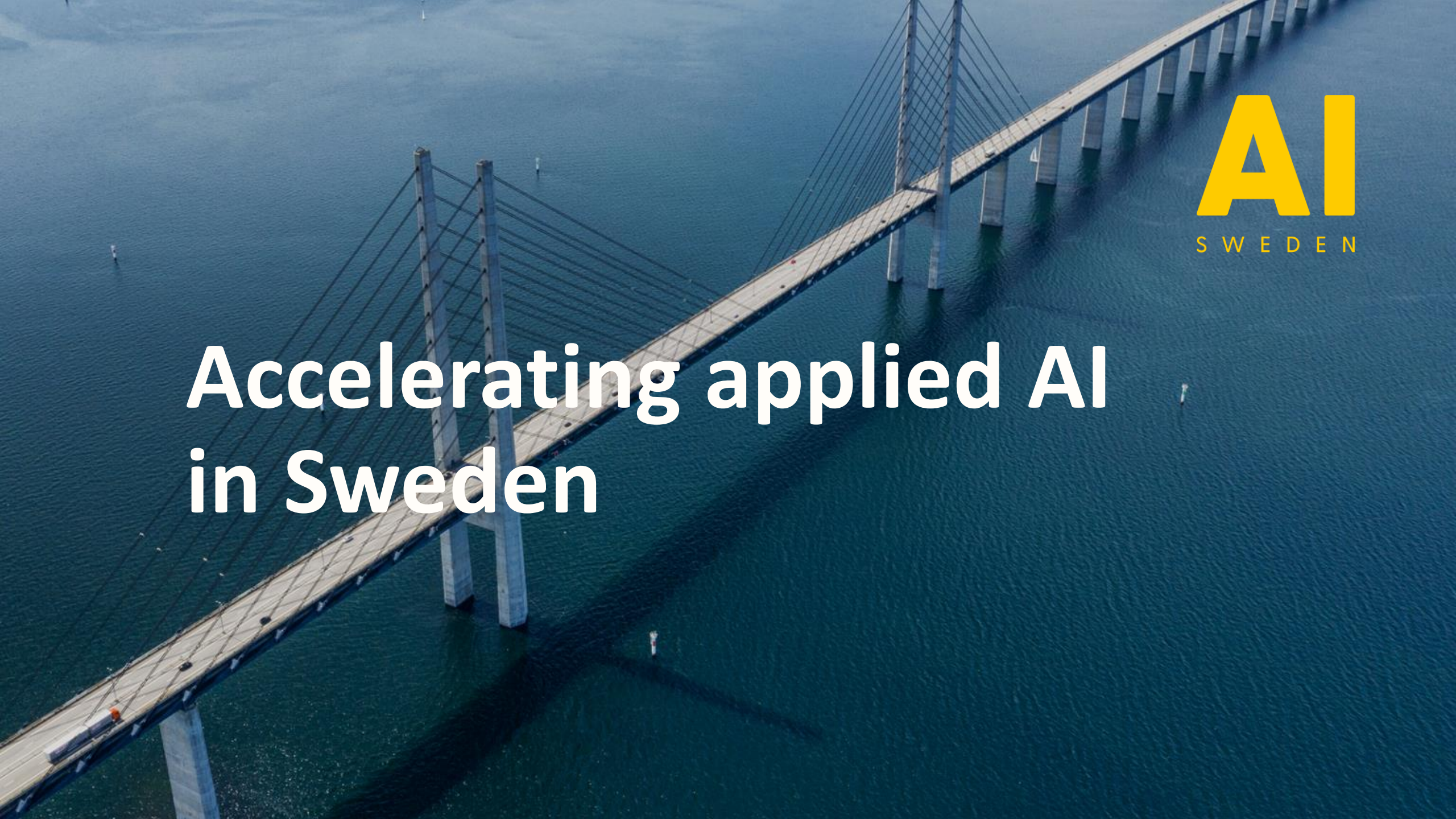


Tillämpad AI

Staffan Truvé

- Varför är jag här?
 - CTO och medgrundare, Recorded Future – ”AI for Intelligence”
 - Ordförande, AI Sweden
 - Ingenjörsvetenskapsakademien (IVA) – ”Peak Human”



Accelerating applied AI in Sweden

Accelerating the use of AI for the benefit of our society, our competitiveness, and for everyone living in Sweden



National center for applied AI

Accelerating applied AI
Swedish industry and
society



Neutral, non-profit and broadly funded

Backed by Swedish
government, by public
and private sector

(~ 100 partners)



Here to help AI help you

Strengthen and
transform operations
through the use of AI

AI
SWEDEN



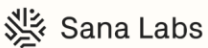
Public sector

Academia



Private sector - SME/Startups

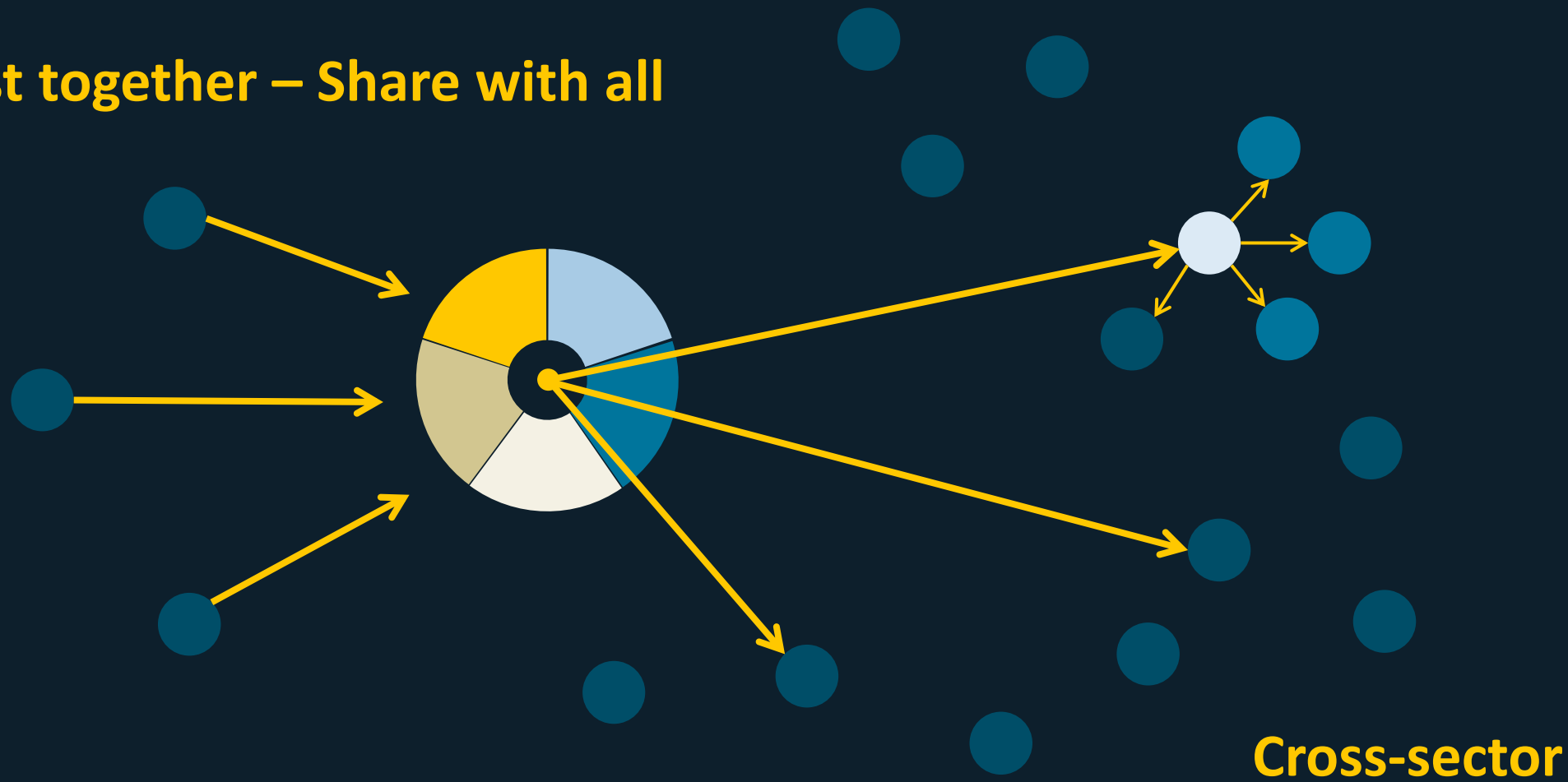
Private sector - Corporate and ME



AKADEMISKA HUS



Invest together – Share with all



Examples of what we do

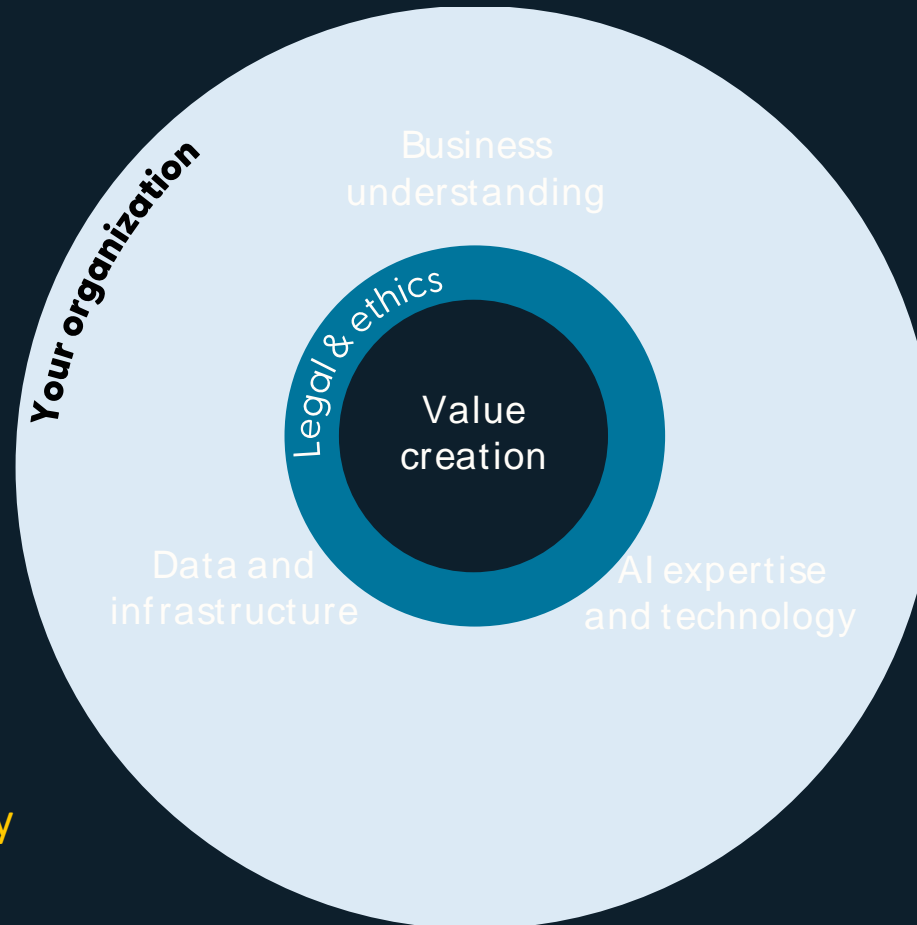
Executive AI Accelerator

Startup program

Legal Expert Group

Data Factory solutions

- Compute and storage capacity
- Infrastructure testbed



AI Change Agent Program

AI for Leaders

Decentralized AI

Language technologies



Strategic areas of applied AI

Decentralized AI

Privacy preserving solutions

Language technologies for Swedish & Other languages

Multi-modal insights & integration

Complex systems management

Organization for AI impact

...

...

Example: Decentralized AI

Investments by partners

Infrastructure
Manpower



Expertise & knowledge sharing

Edge Lab by partners

Use case by partners

Automotive



Healthcare



Recycling



Coming use case: Pharma, security, etc

Research & Innovation partners to be invited

International collaboration – Early discussion initiated



AI for Intelligence

Staffan Truvé ^{PHD}
CTO & Co-Founder
Recorded Future

 Recorded Future[®]

Där all världens information,
transaktioner, IP och pengar bor och
flyttar på sig

GOTT

ONT

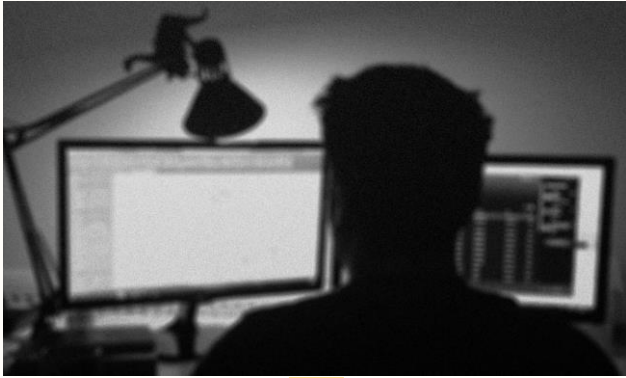
Där cyberattacker planeras, utförs och
kapitaliseras

Grundläggande idéer

- Bygg en riskorienterad tvilling av världen - i Internetskala och i realtid
- Organisera för analys - av människor och algoritmer
- Möjliggör “riskanalys-kentaurer”
- AI för automatisering och förstärkning



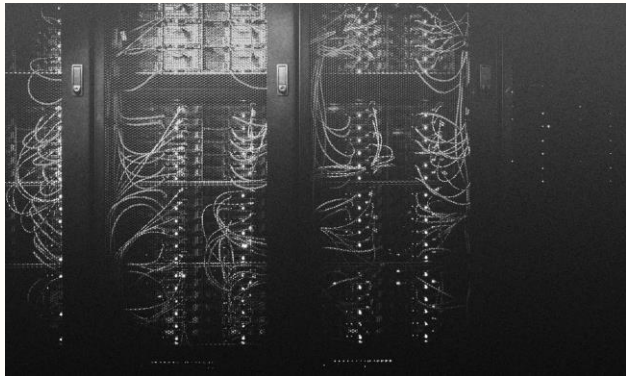
Hur bygger man en digital tvilling?



Unstructured text sources

28 FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals

On Monday, Oct. 26, KrebsOnSecurity began following up on a tip from a reliable source that an aggressive Russian cybercriminal gang known for deploying ransomware was preparing to disrupt information technology systems at hundreds of hospitals, clinics and medical care facilities across the United States. Today, officials from the **FBI** and the **U.S. Department of Homeland Security** hastily assembled a conference call with healthcare industry executives warning about an "imminent cybercrime threat to U.S. hospitals and healthcare providers."

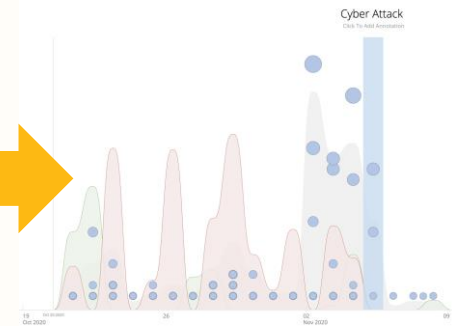
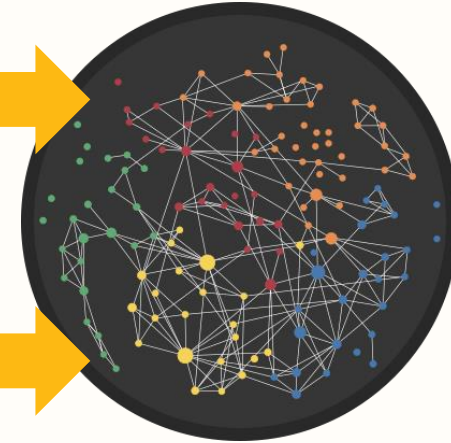


```
2019-12-27 14:58:33.000 59.000 TCP 600 10.255.1.0.11:8180 -> 600 173.17.0.7:5132012 .JP... 0 6 2236 0 300 372 1
2019-12-27 14:58:44.000 5.000 TCP 600 219.254.191.2403 -> 600 1.3.1.0.7:2164087 .JP... 164 13 13144 2 2100 1011 1
2019-12-27 14:58:52.000 0.000 TCP 600 15.1.1.3.5:180 -> 600 1.3.1.0.7:2158103 .JP... 0 1 200 0 0 200 1
2019-12-27 14:58:57.000 0.000 TCP 600 201.223.8.20:180 -> 600 1.3.1.0.7:5146796 .JP... 0 1 522 0 0 522 1
2019-12-27 14:56:04.000 208.000 TCP 600 16.15.111.16:80 -> 600 1.3.1.0.7:107463787 .JP... 164 475 719150 2 27659 1514 1
2019-12-27 14:58:54.000 0.000 TCP 600 173.248.125.23:80 -> 600 1.3.1.0.7:109825 .JP... 0 1 1514 0 0 1514 1
2019-12-27 14:58:32.000 0.000 UDP 600 173.208.165.20:25165 -> 600 1.3.1.0.7:3:59 ..... 0 1 89 0 0 89 1

"sentiments": {
  "classifier_terrorincident_eng": 0.057707563042640686,
  "classifier_cyberattack_eng": 0.04474974051117897
},
"speech_indicator": "speech",
"function": "id",
"binning_id": "DIZ5FgyELu",
"document_offset": 7,
"topics": [
  "P6_kkk",
  "KPzZCG"
],
"analyzed": "2019-03-05T03:04:25.475Z",
```

Structured data from technical sources

Security Intelligence Graph



18.222.171.22 and 64.44.133.143 mentioned

From Twitter by @dmpet

SEP 7 2020 @dmpet Translated from Russian: "Gradually, some details about the attack on SoftServer are beginning to emerge. Thus, 2 IPs appeared in the public domain, from which the attack was supposedly carried out: 64.44.133 [...] 143 18.222.171 [...] 22."

From Twitter by @dmpet on Sep 7, 2020, 16:04

https://twitter.com/dmpet/statuses/1303001099641782272 • Reference Actions • 1+ reference

Open Source Collection

18.222.171.22, #cobaltstrike, #rozena and 4 more mentioned

From Twitter by @JAMESWT_MHT

SEP 10 2020 @JAMESWT_MHT "@malwrhunterteam @VK_intel @bryceabdo related 18.222.171[.]22 #cobaltstrike / #rozena samples https://t.co/r6dG96Ym2q."

From Twitter by @JAMESWT_MHT on Sep 10, 2020, 11:00

Victim Identification



Recorded Future

IP ADDRESS

18.222.171.22

References 25
First Reference Sep 7, 2020
Latest Reference Oct 25, 2020
ASN AS16509
ORG AMAZON-02
GEO Columbus, United States

41
SUSPICIOUS RISK SCORE
6 of 53 Risk Rules Triggered

TRIGGERED RISK RULES

- Recent C&C Server • 1 sighting on 1 source
Recorded Future Command & Control List. Command & Control host identified on Oct 25, 2020.
- Current C&C Server • 1 sighting on 1 source
Cobalt Strike Default Certificate Detected - Shodan / Recorded Future. Mitigated by being in Amazon Web Services Infrastructure (White List).

Risk Scoring

IP ADDRESS

192.240.46.47

References 0

IP Address 192.240.46.47
Type IPv4
WHOIS http://whois.domaintools.com/192.240.46.47
ASN AS26385 THE-UNIVERSITY-OF-VERMONT-MEDICAL-CENTER-1
Country United States of America

Unread Priority Alerts

38

38 unread of 47 priority alerts in the last 7 days

Alerting

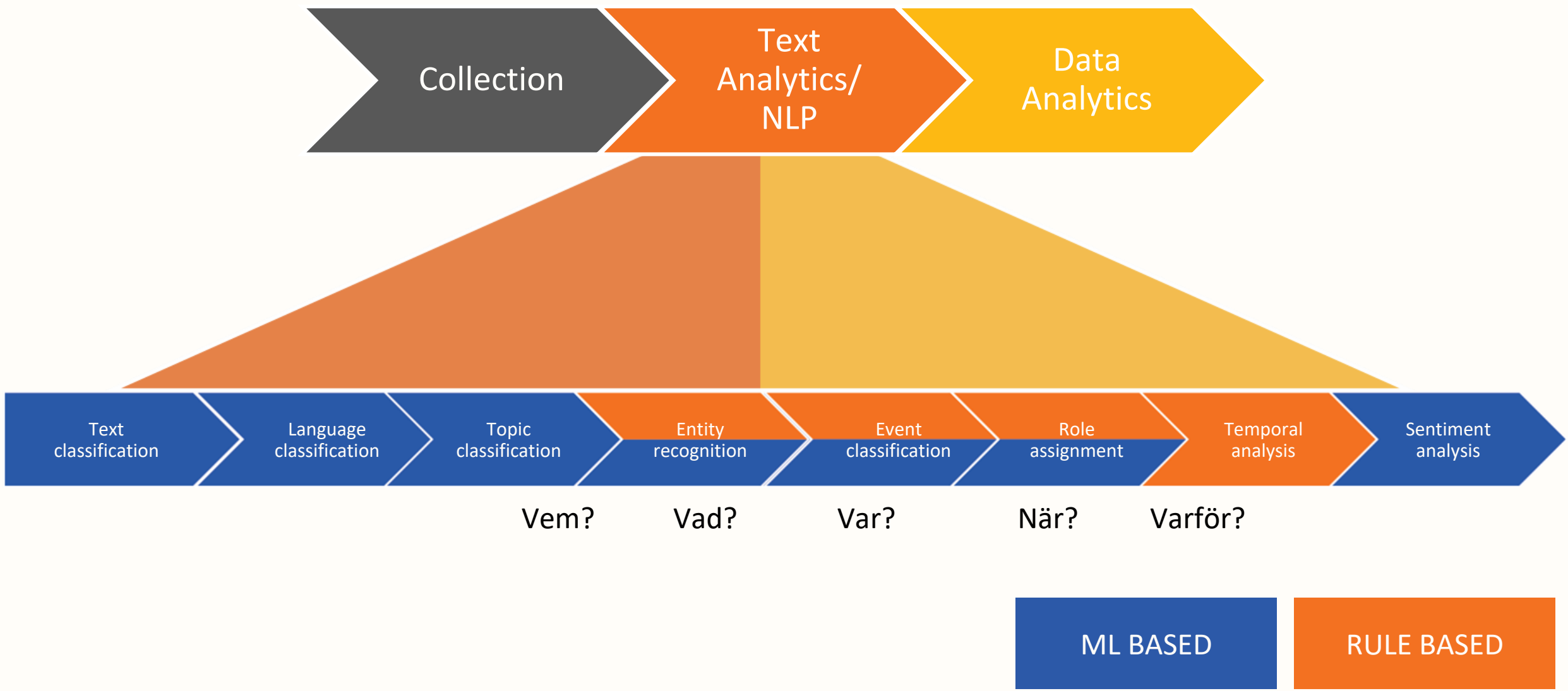


First seen → Last seen	Date ↑	Org	Category	Type	Value	Tags
	2020-11-05		Network activity	ip-dst port	18.222.171.22:443	recorded-future:infra="C2" x
	2020-10-28T22:18:21.000000+00:00		Network activity	ip-src	192.240.46.47	recorded-future:victim x
	2020-10-28T23:25:03.000000+00:00					

Targeted Collection

AI @ Recorded Future

- Kunskapsrepresentation – Security Intelligence Graph
- Textanalys / NLP
- Risk Scoring / Anomalidetektering
- Prediktiv Analys



Event Extraction

Petya Cyber attack against Hospitals by Russia in Europe

FEB
16
2018

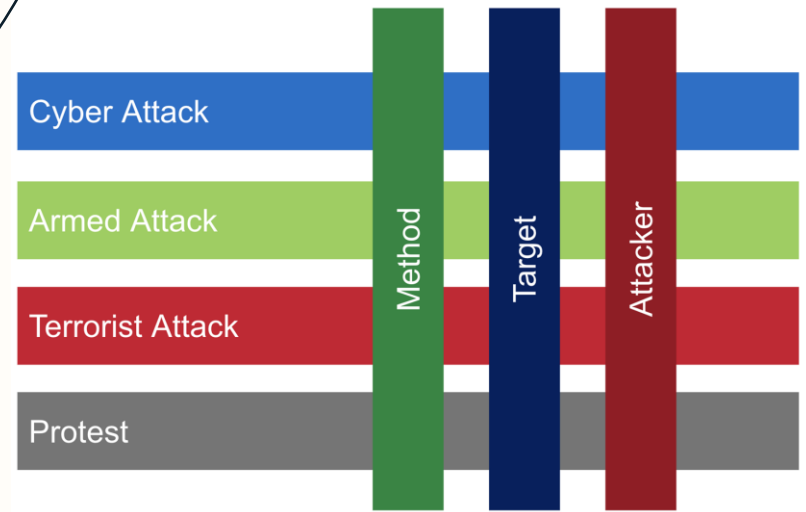
From Twitter by @AdeptcoreInc

@AdeptcoreInc "U.K. says Russia was behind #Petya #cyberattack that shut down Nuance, #hospitals <https://t.co/AnXXlsuEAn> <https://t.co/plaCwZNQKp>."

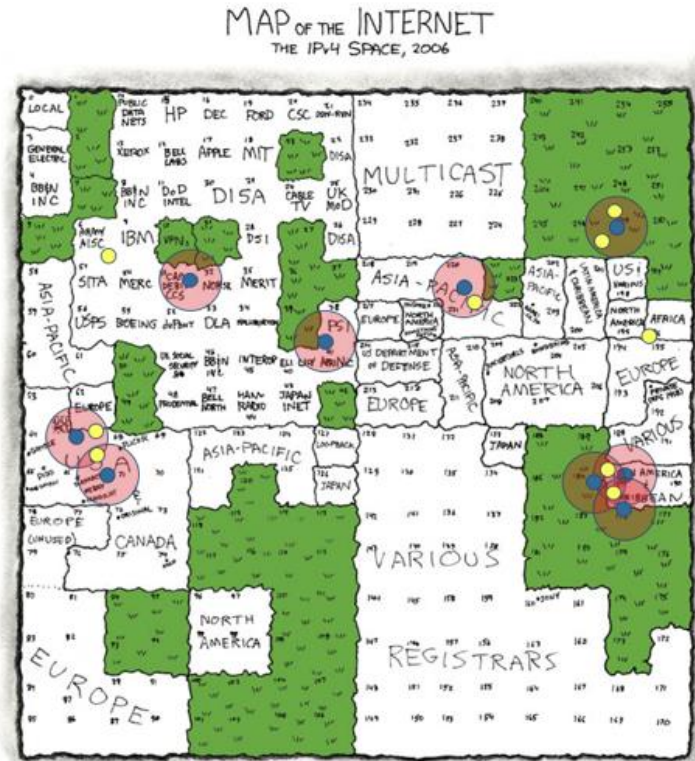
From Twitter by @AdeptcoreInc on Feb 16, 2018, 15:19

CyberAttack
Attacker
Target
Method
Operation
RelatedEntities
...

- Country: Russia
- Company: Nuance
- Industry: Hospitals
- Malware: Petya
- Country: United Kingdom



Exempel: prediktering av IP-risk

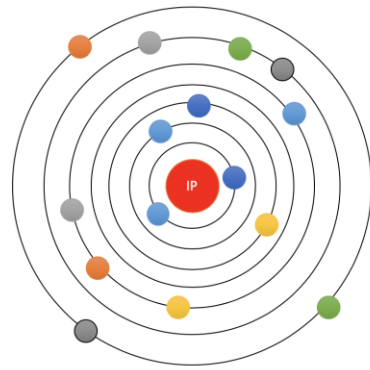


THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING-- ANY CONSECUTIVE STRING OF IPs WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IPs THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

0 1 14 15 16 19 →
3 2 13 12 17 18
4 7 8 11
5 6 9 10

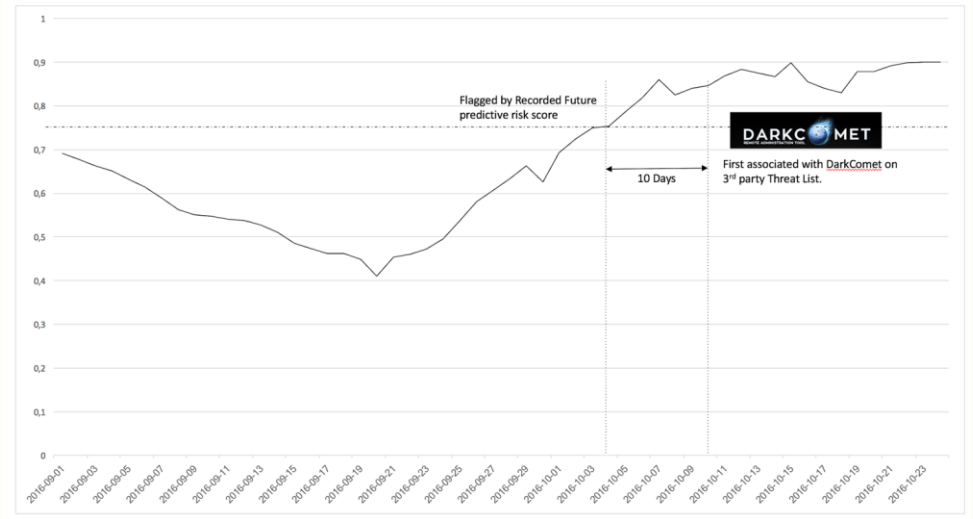
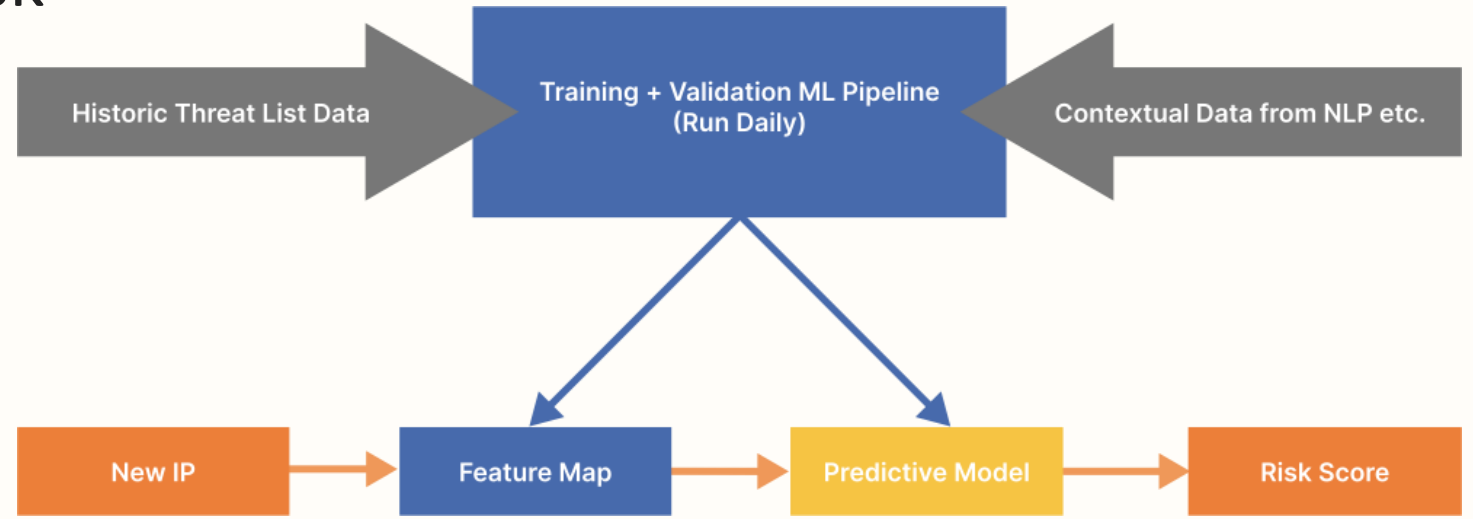


= UNALLOCATED BLOCK



→ Growing CIDR distance from reference IP

- Variety of tracked threat lists
- IP white lists
- IPs mentioned on Twitter
- IPs mentioned on Twitter as the source of an attack
- IPs mentioned on Pastebin
- IPs mentioned on Pastebin in connection to malware
- ...



Slutsatser

- AI kan verkligen ge företag unika konkurrensfördelar
- Inte en lösning i sig, utan som del i en systemlösning
- AI erbjuder en portfölj av verktyg – representation, logik, ML
- Kentaurer: människa + maskin
- Vi har knappt ens börjat...



Dynabook,
1968

The best way to predict the future is
to invent it! (Alan Kay, 1971)

Staffan Truvé
truve@recordedfuture.com