USE OF AI IN OPERATIONAL TECHNOLOGY NETWORKS AND PACKET-BASED ATTACKS DETECTION

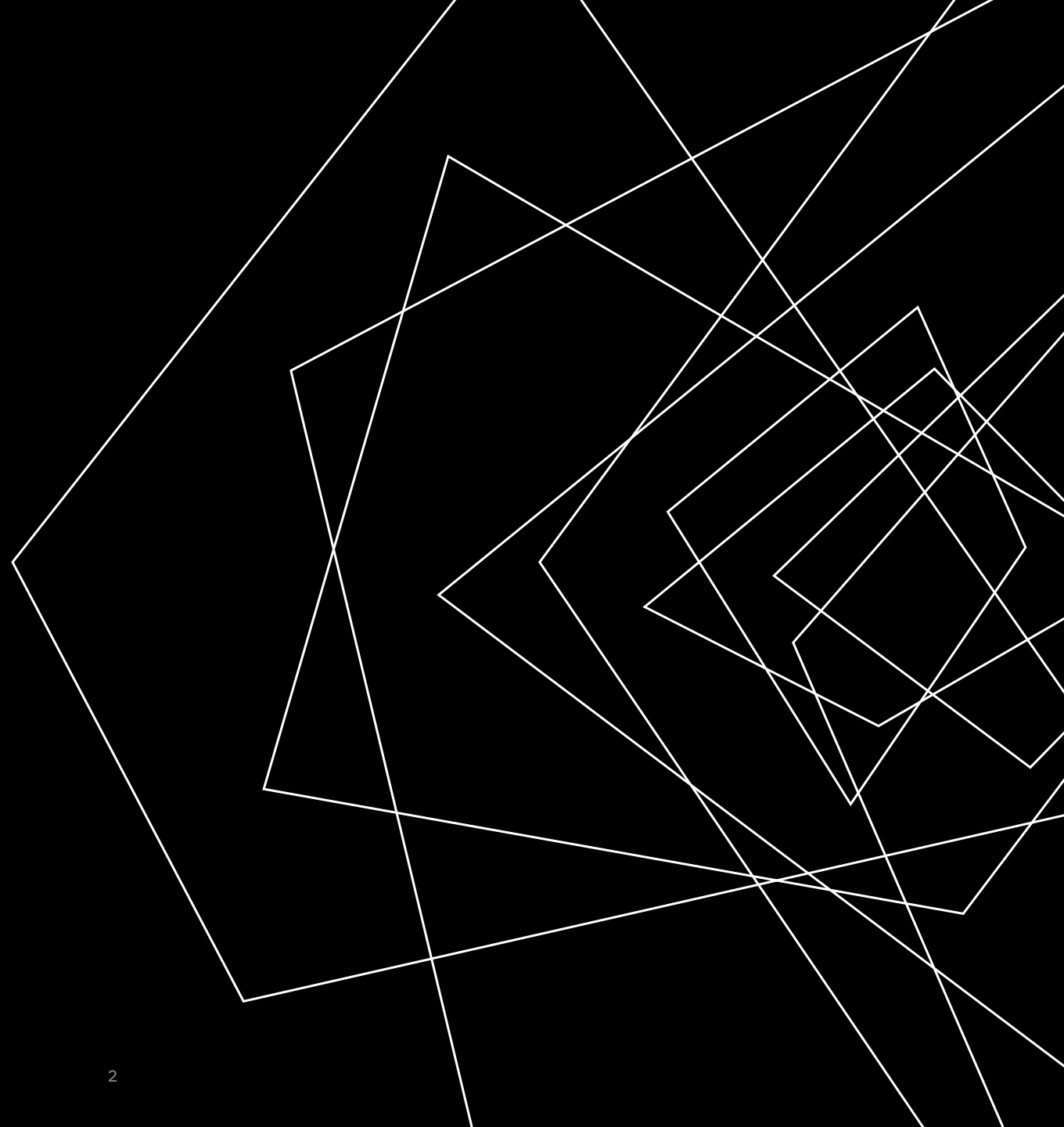
Zoltan Dobrady, Szilard Takacs, Timot Hidvegi

ABOUT US

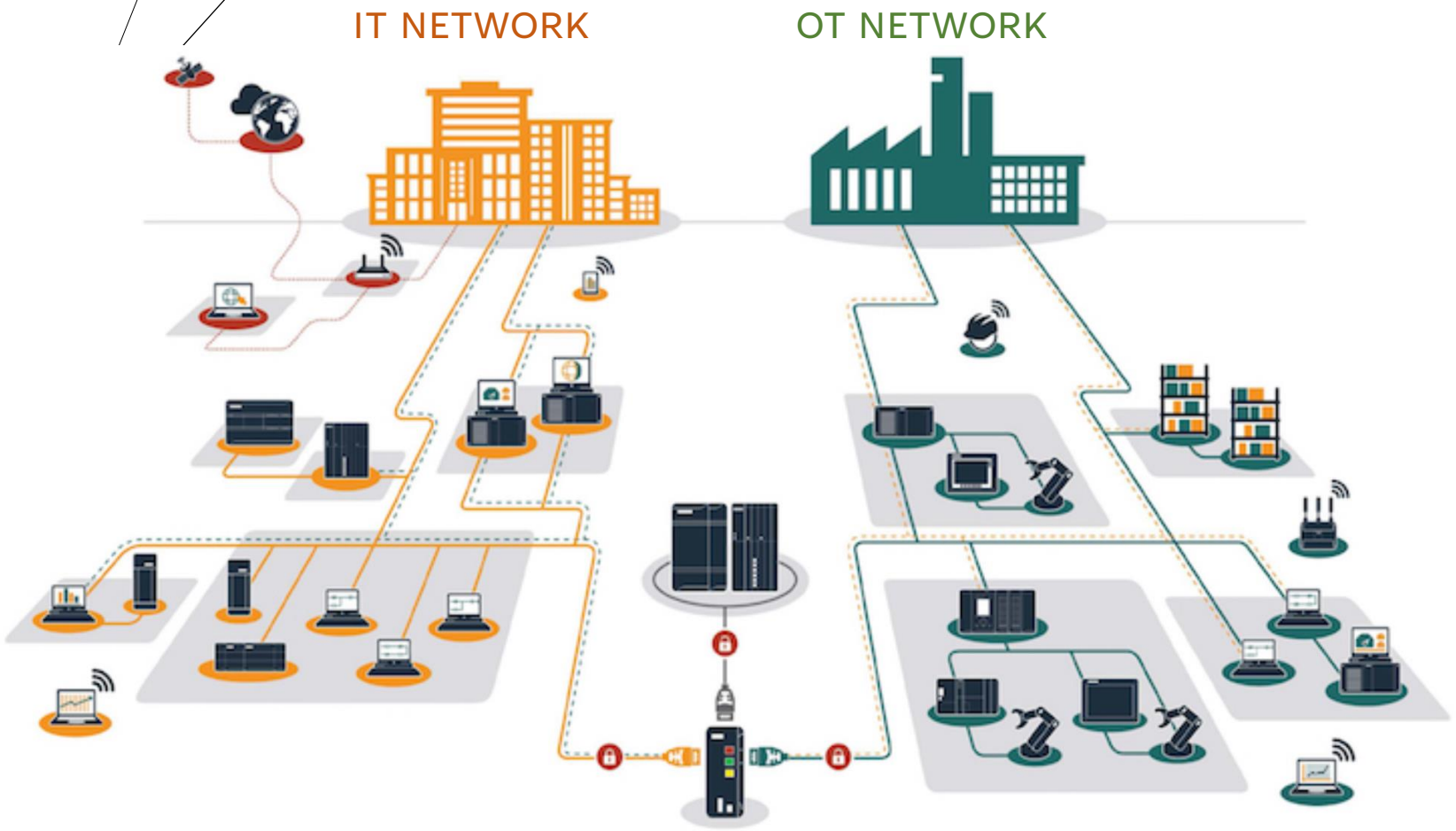
„Industrial and Research Lab for Cybersecurity”

Research area:

Artificial intelligence applied to automotive and industrial systems.



NETWORK OVERVIEW



- OT network = Hálózatba kötött ipari gyártósori eszközök
  Kutatásunk az ezen hálózaton folyó adatcsomagokat elemzi
- Ezen zajlik a gépegységek közötti kommunikáció
- Bele tartozik a géphez tartozó perifériák kommunikációja is (pl ProfiNET, ProfiBUS, stb)

Source: TechPaper: What to expect when analyzing an OT network - Inprosec

PROBLEM

VULNERABILITY

OT systems or networks may be susceptible to targeted cyberattacks
Contrary to IT systems, these peripherals are not intended to ward off cyberattacks

PRODUCTION DOWNTIME

Current example: Recently one big car manufacture acknowledged to suffer a targeted cyberattack witch caused the complette stop off production lines across Europe.

DEFECTIVE PRODUCT MANUFACTURING

Even one manipulated data packet is enough to cause a peripheral to malfunction. This leads to the production of defective products, which causes a lot of financial costs.

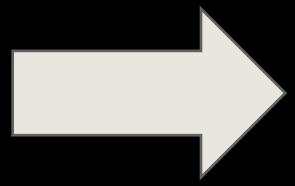
DATA PACKET ANALYSIS

Currently this datapacket analisys is done manually after the attack with filtering methods(e.g. wireshark,)
which poses an additional error source, and it takes a great deal of time

POSSIBLE SOLUTION

„Real time” analysis

It is imperative that the packets are analyzed in real time, rather than after the attack has occurred.



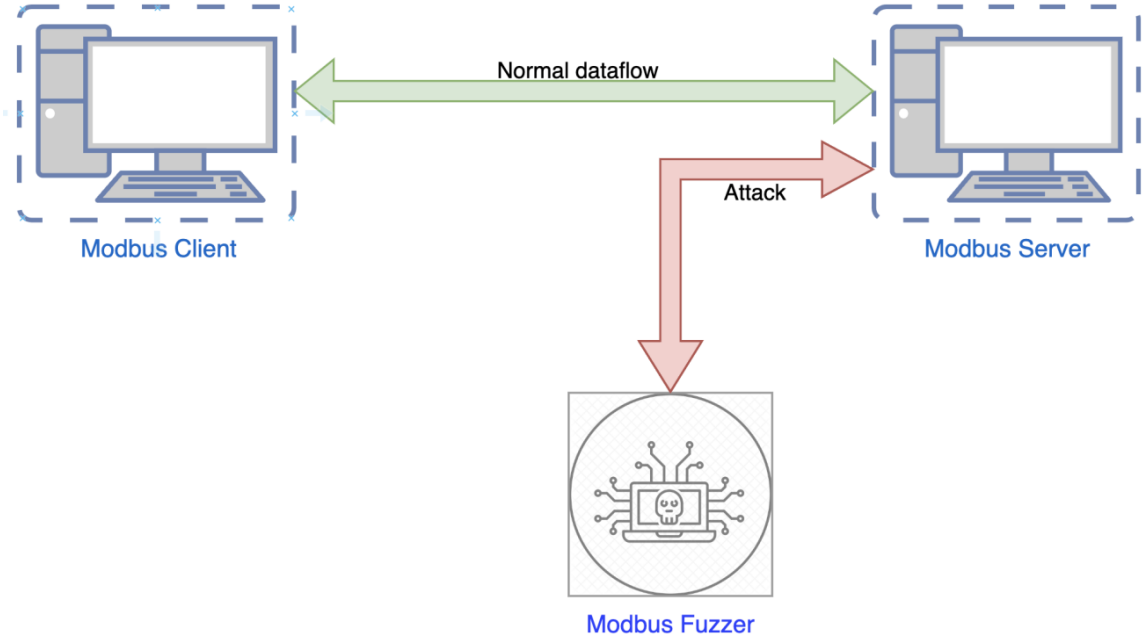
Use of Artifical itelligent

After selecting the appropriate learning method for the A.I., packet analysis can be used to predict attacks

VIRTUAL TESTING ENVIROMENT

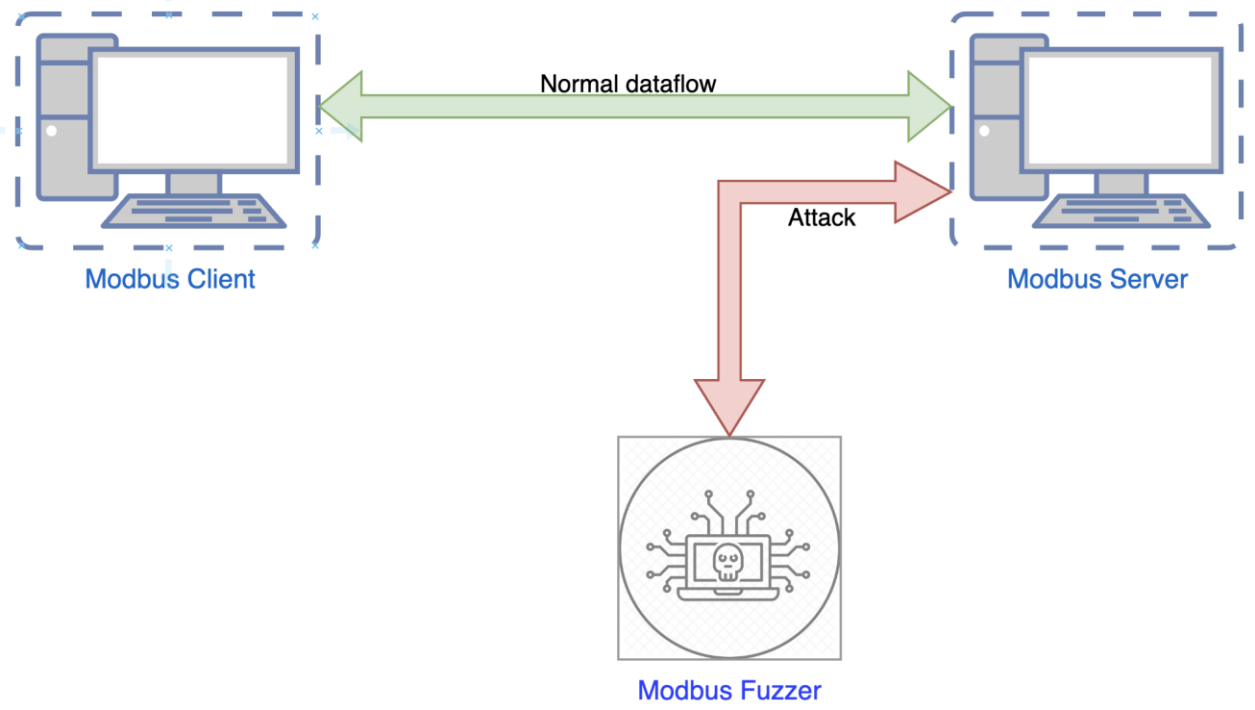
Simulated OT network datafow for TCP/IP modbusprotocoll

Attacking with an fuzzer

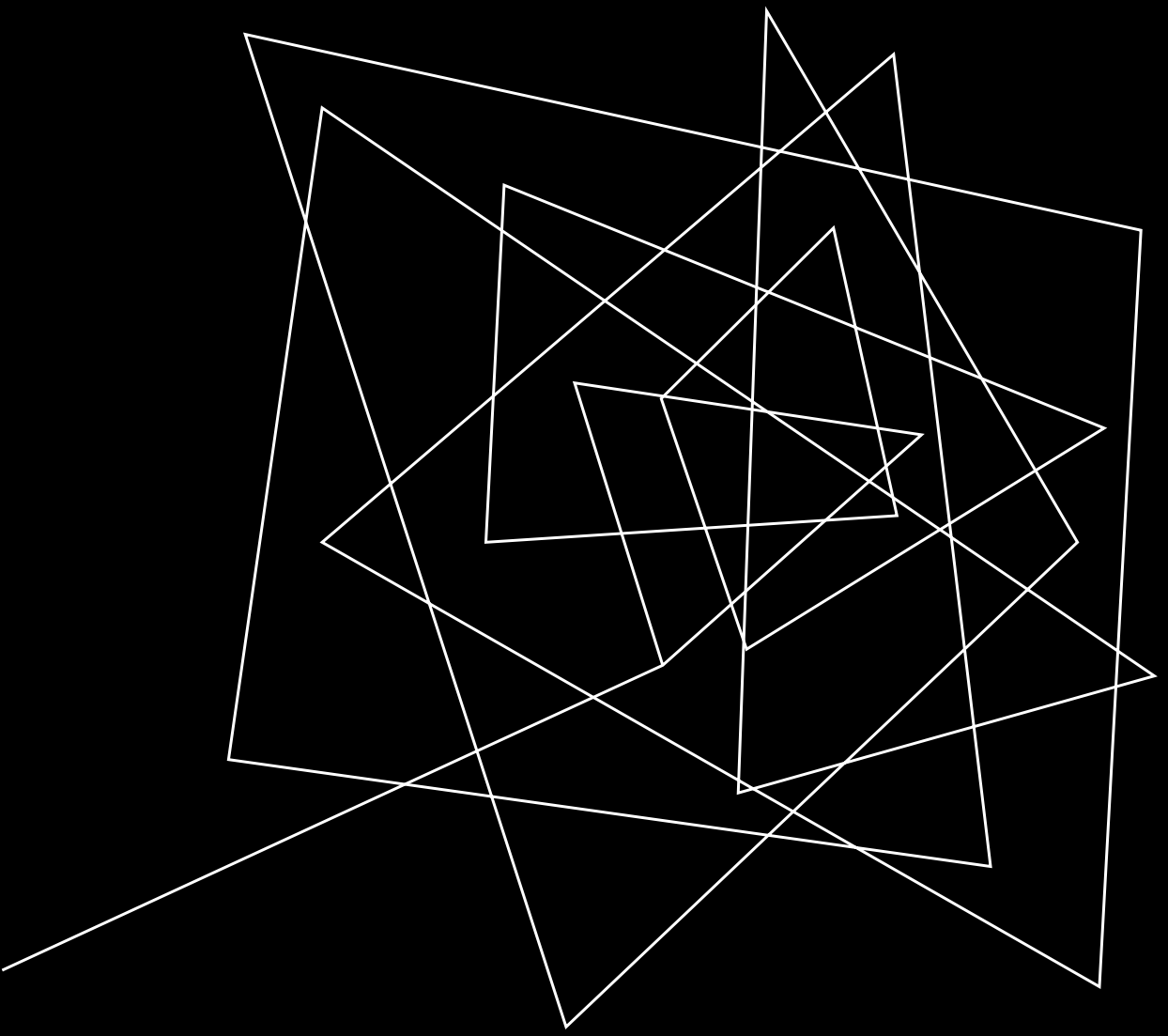


ATTACKING MECHANISM

- Flooding the datastream with large amounts of data
- In response the server is left with little or no resource for communication to the client



A.I.



- ARTIFICIAL INTELLIGENCE, REFERS TO THE SIMULATION OF HUMAN INTELLIGENCE IN MACHINES THAT ARE PROGRAMMED TO THINK AND LEARN LIKE HUMANS.

  WE USED LOT OF AI METHODS LIKE NATURAL LANGUAGE PROCESSING, AND STATISTICAL LEARNING

PREPARING GENERATED DATA FOR A.I.

- The generated data packets are labelled
- Irrelevant columns have been deleted.
- Applied word-based tokenization on the 'data' column
- Created embeddings to construct the training dataset,
- which could be processed by the language models.

Before:

	Source	Destination	Protocol	Length	Info
0	PcsCompu_22:46:4f	Broadcast	ARP	60	Who has 192.168.56.113? Tell 192.168.56.114
1	PcsCompu_75:69:b0	PcsCompu_22:46:4f	ARP	42	192.168.56.113 is at 08:00:27:75:69:b0
2	192.168.56.114	192.168.56.113	TCP	74	36610 > 502 [SYN] Seq=0 Win=64240 Len=0 MSS=...
3	192.168.56.113	192.168.56.114	TCP	74	502 > 36610 [SYN, ACK] Seq=0 Ack=1 Win=65160...
4	192.168.56.114	192.168.56.113	TCP	66	36610 > 502 [ACK] Seq=1 Ack=1 Win=64256 Len=...
...	...	...	...	...	...
430913	13.229.250.8	192.168.56.113	TCP	54	1234 > 502 [SYN] Seq=0 Win=8192 Len=0
430914	224.168.77.124	192.168.56.113	TCP	54	1234 > 502 [SYN] Seq=0 Win=8192 Len=0
430915	130.136.216.64	192.168.56.113	TCP	54	1234 > 502 [SYN] Seq=0 Win=8192 Len=0
430916	82.246.78.254	192.168.56.113	TCP	54	1234 > 502 [SYN] Seq=0 Win=8192 Len=0
430917	139.102.116.152	192.168.56.113	TCP	54	1234 > 502 [SYN] Seq=0 Win=8192 Len=0

430918 rows × 6 columns

After:

Data				IsAttack?
Source IP	Destination IP	Protocol	Length	(0 = No attack,1 = Attack)
210.11.140.185	192.168.56.113	TCP	54	1
14.221.153.215	192.168.56.113	TCP	54	1
176.137.215.247	192.168.56.113	TCP	54	1
88.64.227.9 192	192.168.56.113	TCP	60	0
3.156.6.135 192	192.168.56.113	TCP	60	0

RESULT AND ANALYSIS ON STATISTICAL LEARNING MODE

Models	Accuracy score
Linear regression	0.443869
Logistic regression	69.04627
kNN(k Nearest Neighbors)	31.23024
Linear Discriminant Analysis	68.80032
Quadratic Discriminant Analysis	68.75143
Support Vector Machine	69.04627
Naive Bayes	69.04627
Random Forest	46.13880

ABSTRACT

We based our research on market trends and social media

DESIGN

We believe people need more products specifically dedicated to this niche market

RESEARCH

Minimalist and easy to use

MARKET OVERVIEW

£3 BILLION

Freedom to invent

Selectively inclusive market

Serviceable available market

£1 BILLION

Opportunity to build

Fully inclusive market

Total addressable market

£2 BILLION

Few competitors

Specifically targeted market

Serviceable obtainable market

MARKET COMPARISON

OPPORTUNITY TO BUILD

Addressable market

FREEDOM TO INVENT

Serviceable market

FEW COMPETITORS

Obtainable market

OUR COMPETITION

CONTOSO

Our product is priced below that of other companies on the market

Design is simple and easy to use, compared to the complex designs of the competitors

Affordability is the main draw for our consumers to our product

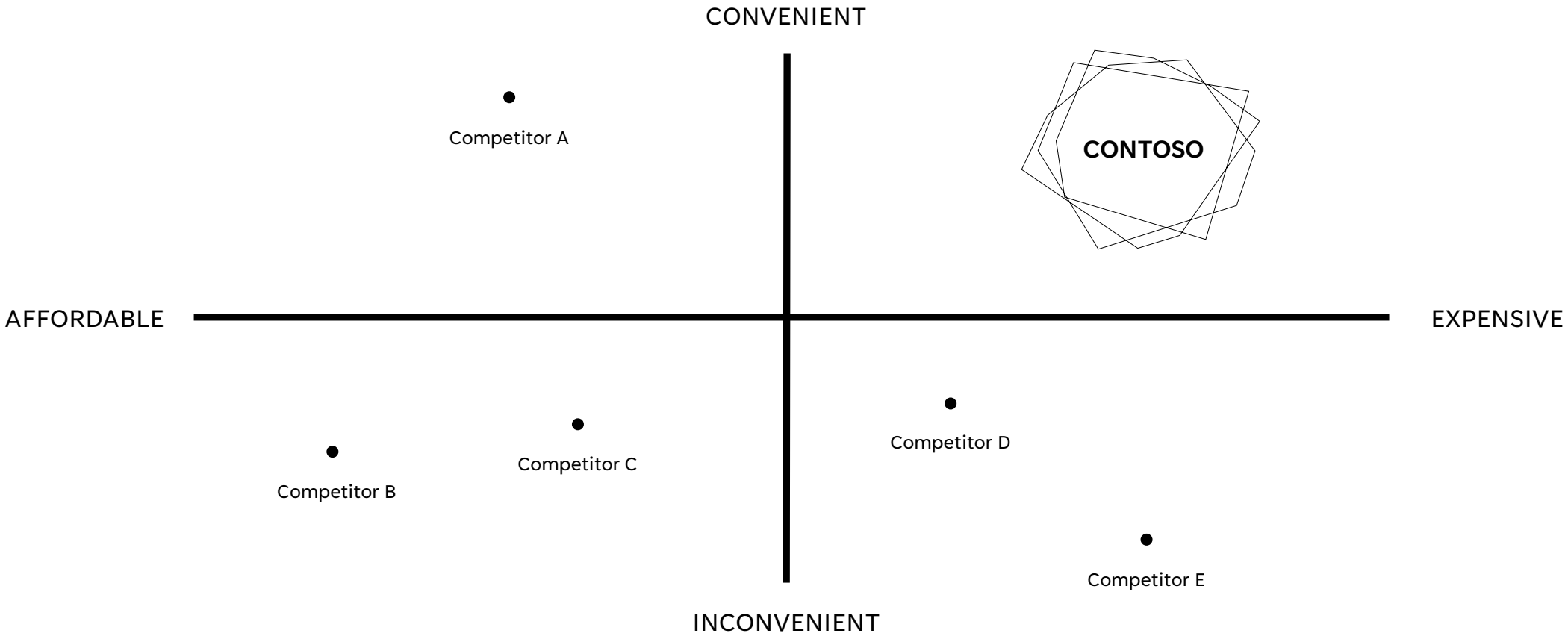
COMPETITORS

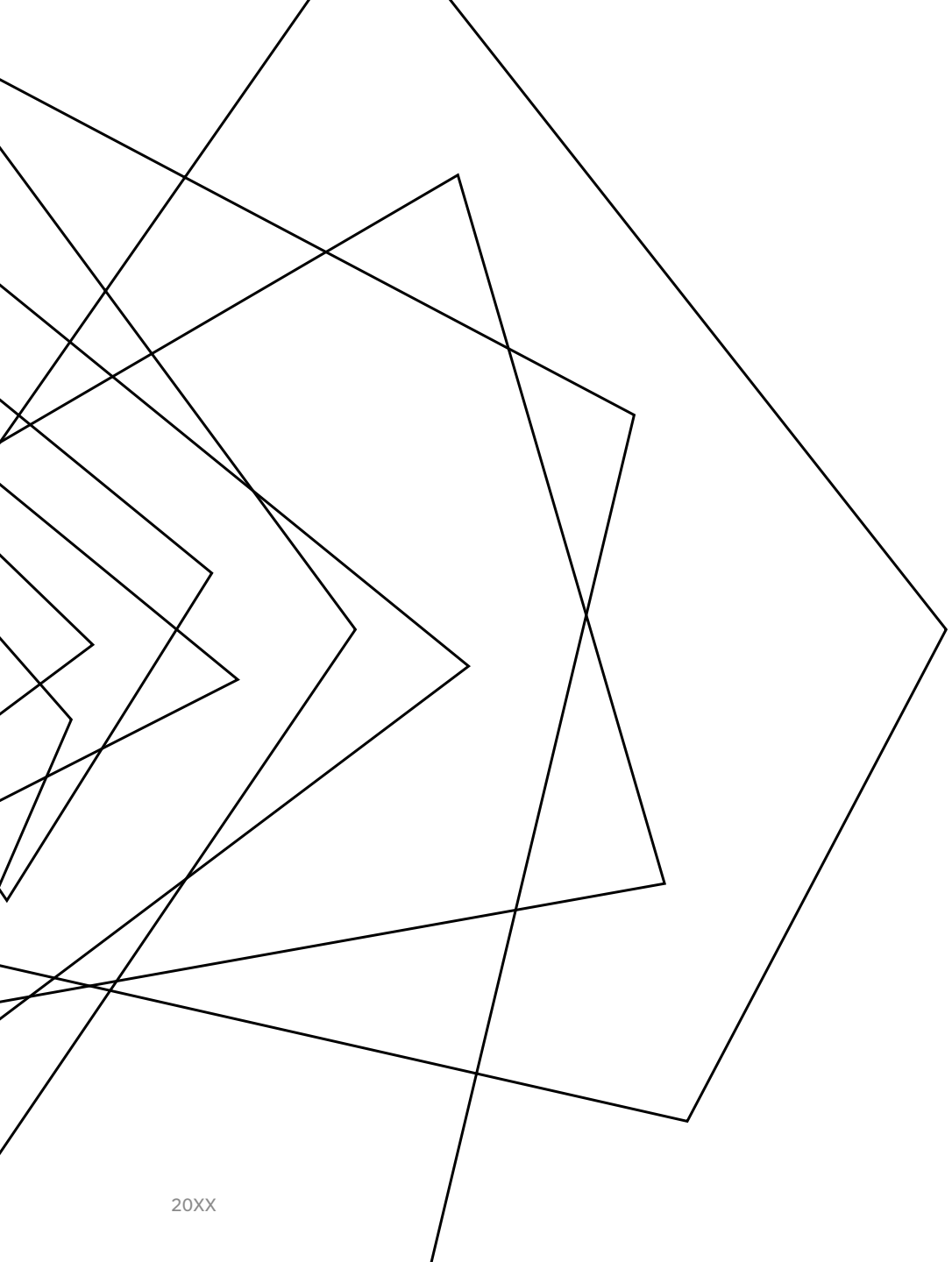
Company A
Product is more expensive

Companies B & C
Product is expensive and inconvenient to use

Companies D & E
Product is affordable, but inconvenient to use

OUR COMPETITION





GROWTH STRATEGY

FEB 20XX

Roll out product to high profile or top-level participants to help establish the product

MAR 20XX

Release the product to the general public and monitor press release and social media accounts

OCT 20XX

Gather feedback and adjust product design as necessary

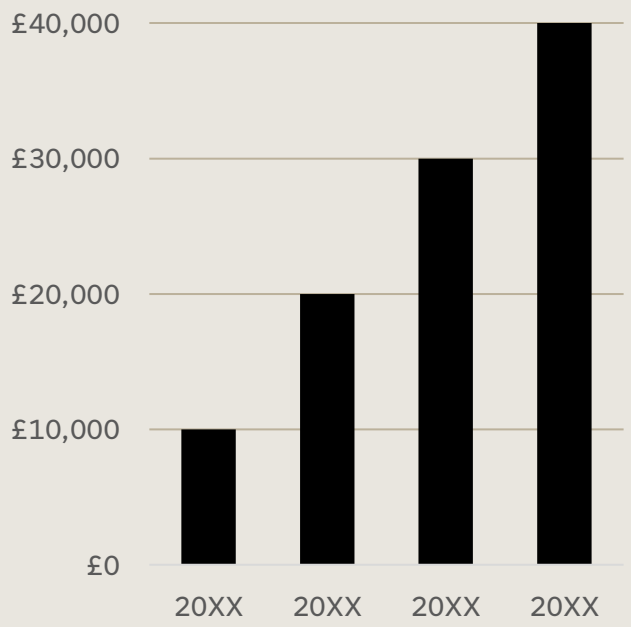
TRACTION

Forecasting for success

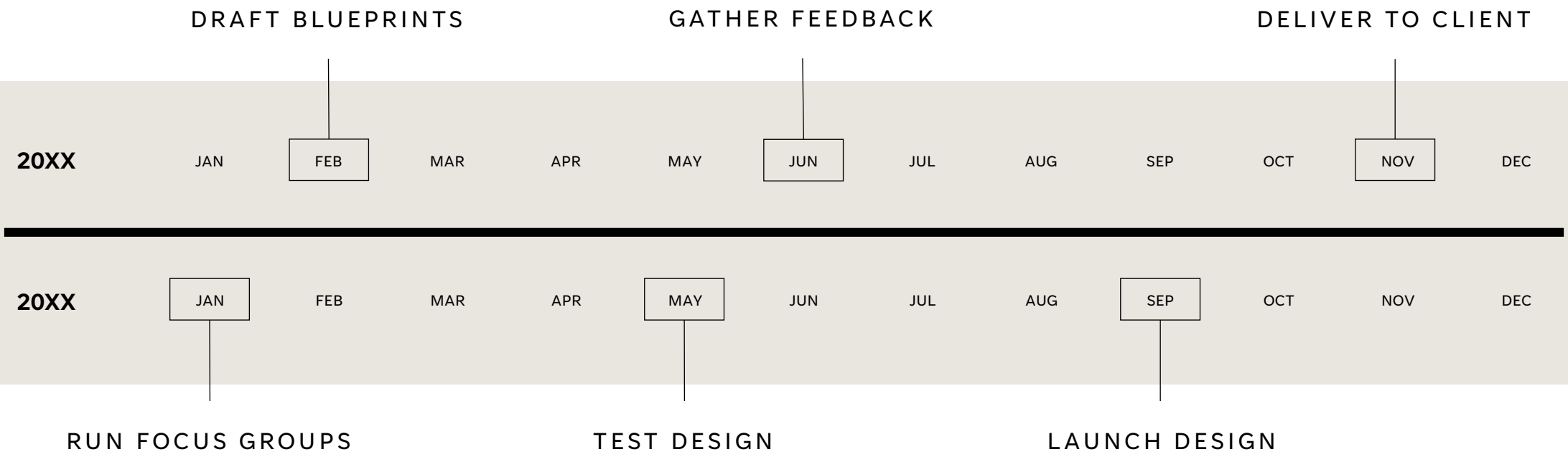
KEY METRICS

	Clients	Orders	Gross revenue	Net revenue
20XX	10	1100	£10,000	£7,000
20XX	20	200	£20,000	£16,000
20XX	30	300	£30,000	£25,000
20XX	40	400	£40,000	£30,000

REVENUE BY YEAR



TWO-YEAR ACTION PLAN



FINANCIALS

	Year 1	Year 2	Year 3	
INCOME				
Users	50,000	400,000	1,600,000	
Sales	500,000	4,000,000	16,000,000	
Average price per sale	75	80	90	
Revenue @ 15%	5,625,000	48,000,000	216,000,000	
GROSS PROFIT	**5,625,000**	**48,000,000**	**216,000,000**	
Expenses				
Sales & marketing	5,062,500	38,400,000	151,200,000	70%
Customer service	1,687,500	9,600,000	21,600,000	10%
Product development	562,500	2,400,000	10,800,000	5%
Research	281,250	2,400,000	4,320,000	2%
TOTAL EXPENSES	**7,593,750**	**52,800,000**	**187,920,000**	

MEET THE TEAM

TAKUMA HAYASHI

President

MIRJAM NILSSON

Chief Executive Officer

FLORA BERGGREN

Chief Operations Officer

RAJESH SANTOSHI

VP Marketing

MEET THE TEAM

TAKUMA HAYASHI
President

MIRJAM NILSSON
Chief Executive Officer

FLORA BERGGREN
Chief Operations Officer

RAJESH SANTOSHI
VP Marketing

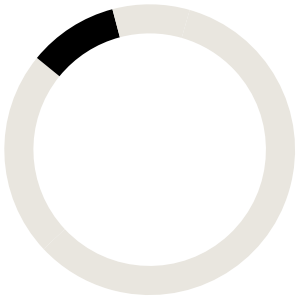
GRAHAM BARNES
VP Product

ROWAN MURPHY
SEO Strategist

ELIZABETH MOORE
Product Designer

ROBIN KLINE
Content Developer

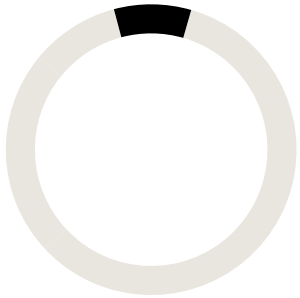
FUNDING



£14,000

ANGEL INVESTMENTS

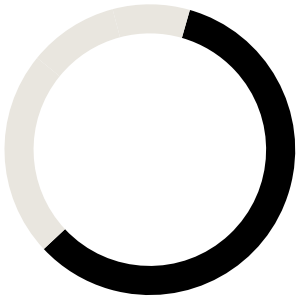
Amount obtained through other investors



£12,000

PROPERTY

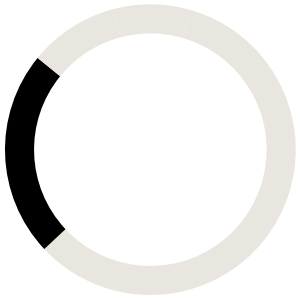
Revenue obtained from property rentals



£82,000

SHARES

Number of shares converted into USD



£32,000

CASH

Liquid cash we have on hand

SUMMARY

At Contoso, we believe in giving 110%. By using our next-generation data architecture, we help organisations virtually manage agile workflows. We thrive because of our market knowledge and great team behind our product. As our CEO says, "Efficiencies will come from proactively transforming how we do business."

- Megelőzhető?

- Kutatásunk erre a kérdésre keresi a választ, hogy hogyan tudjuk erre a feladatra a mesterséges inteligenciát felhasználni. További céljaink, az adott támadási mechanizmusok prediktálása.

THANK YOU

Mirjam Nilsson

206-555-0146

mirjam@contoso.com

www.contoso.com