Hochschule Worms
University of Applied Sciences

Network

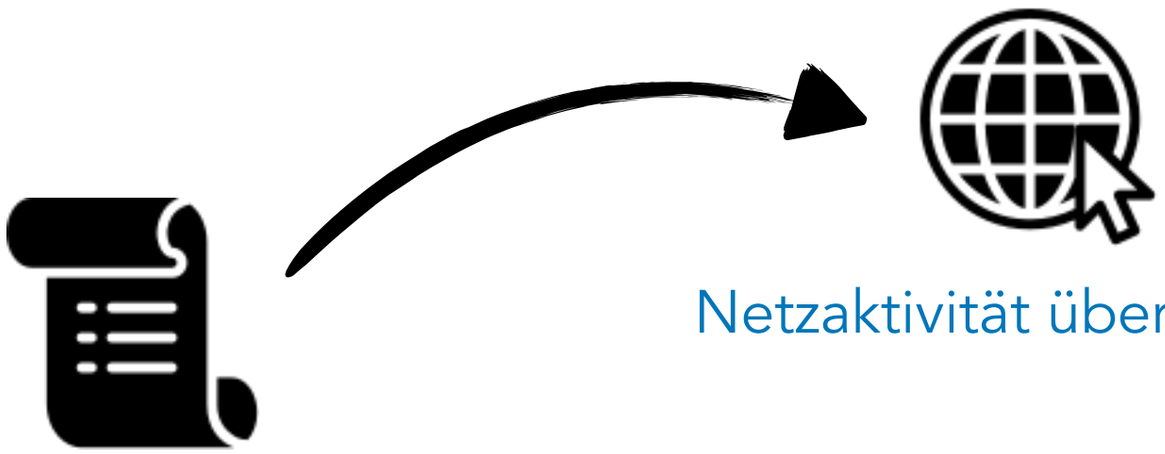
ANOMALY DETECTION

Lucas Elsässer

Signature-based IDS

Rule based

Signature-based IDS



Netzaktivität überwachen

Rule based

Signature-based IDS

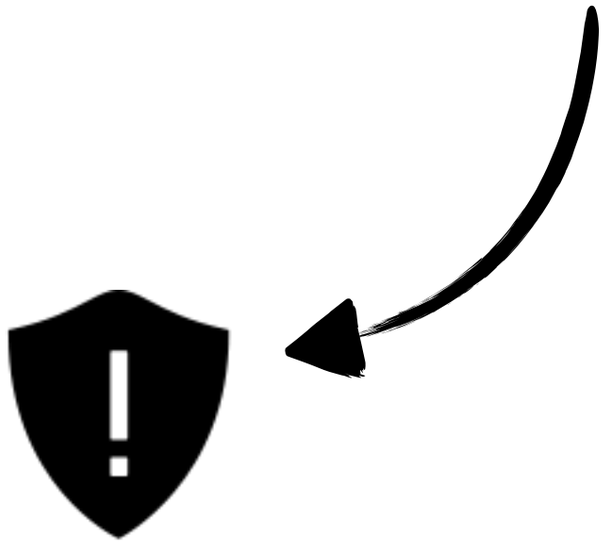
Rule based

Signatur abgleich

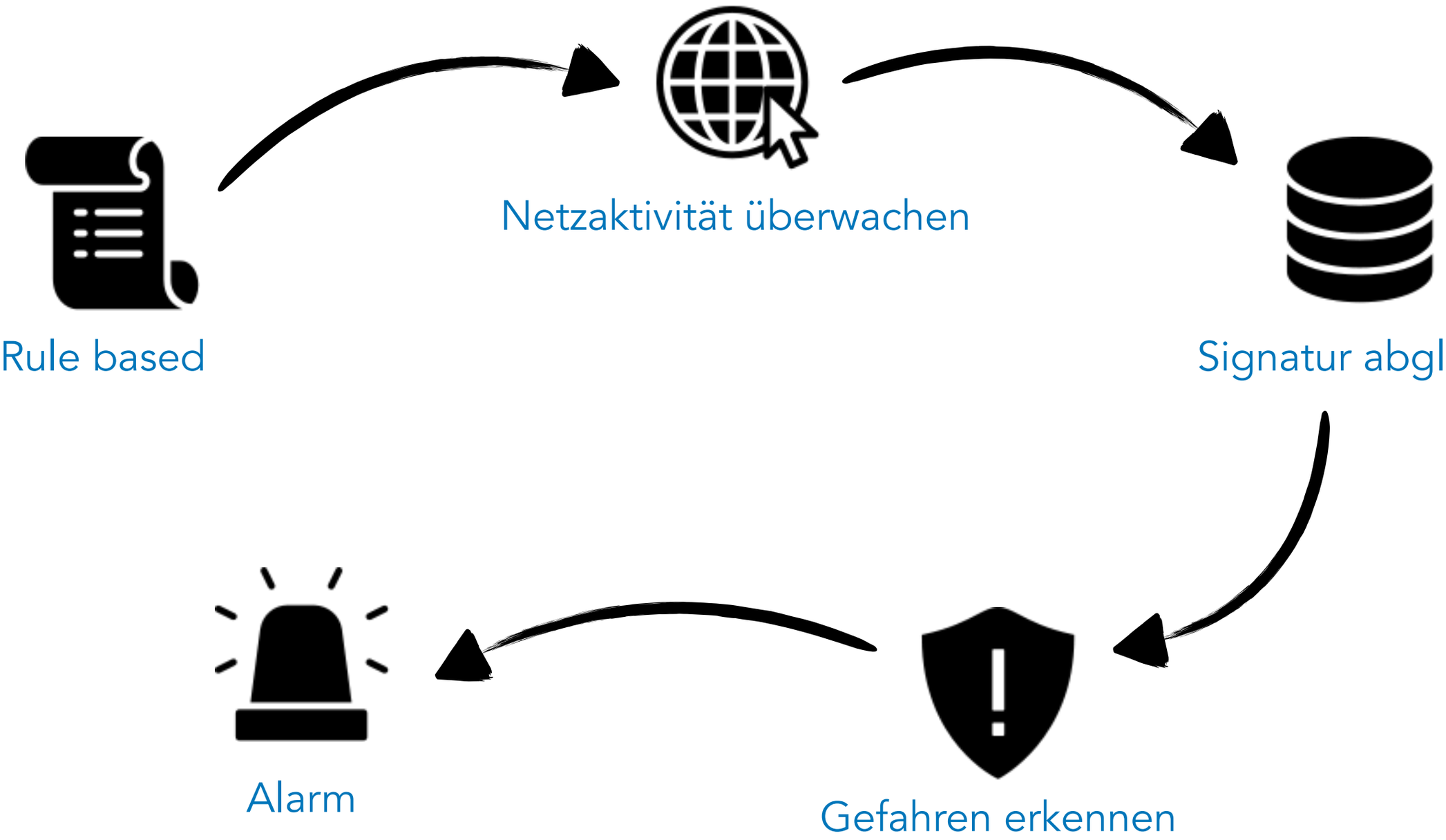
Signature-based IDS

Rule based

Signatur abgleich



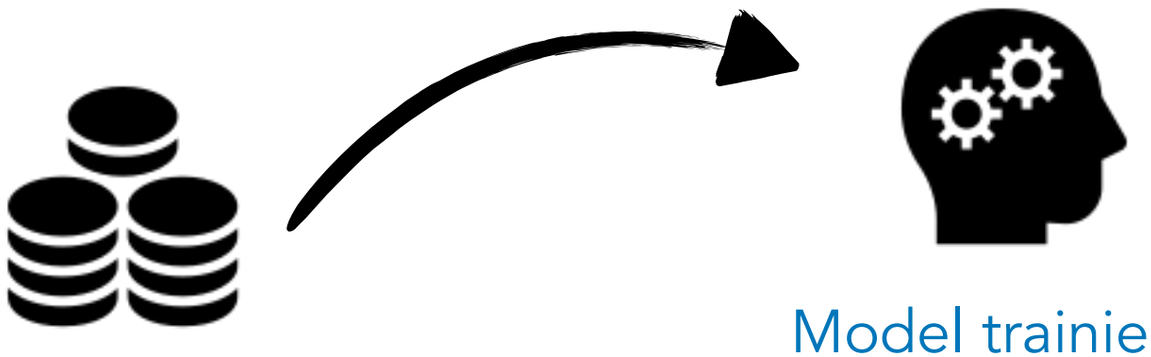
Signature-based IDS



Anomaly-based IDS

Datenmenge

Anomaly-based IDS



Model trainieren

Datenmenge

Anomaly-based IDS

Datenmenge

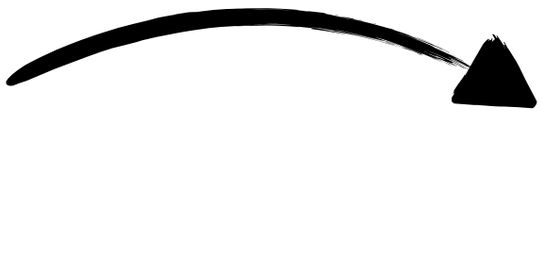
Model trainieren

Netzaktivität überwachen

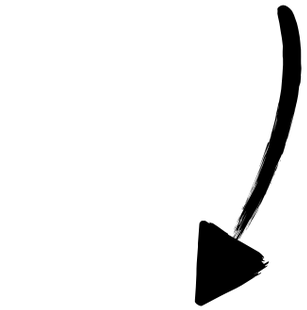
Anomaly-based IDS

Datenmenge

Model trainieren

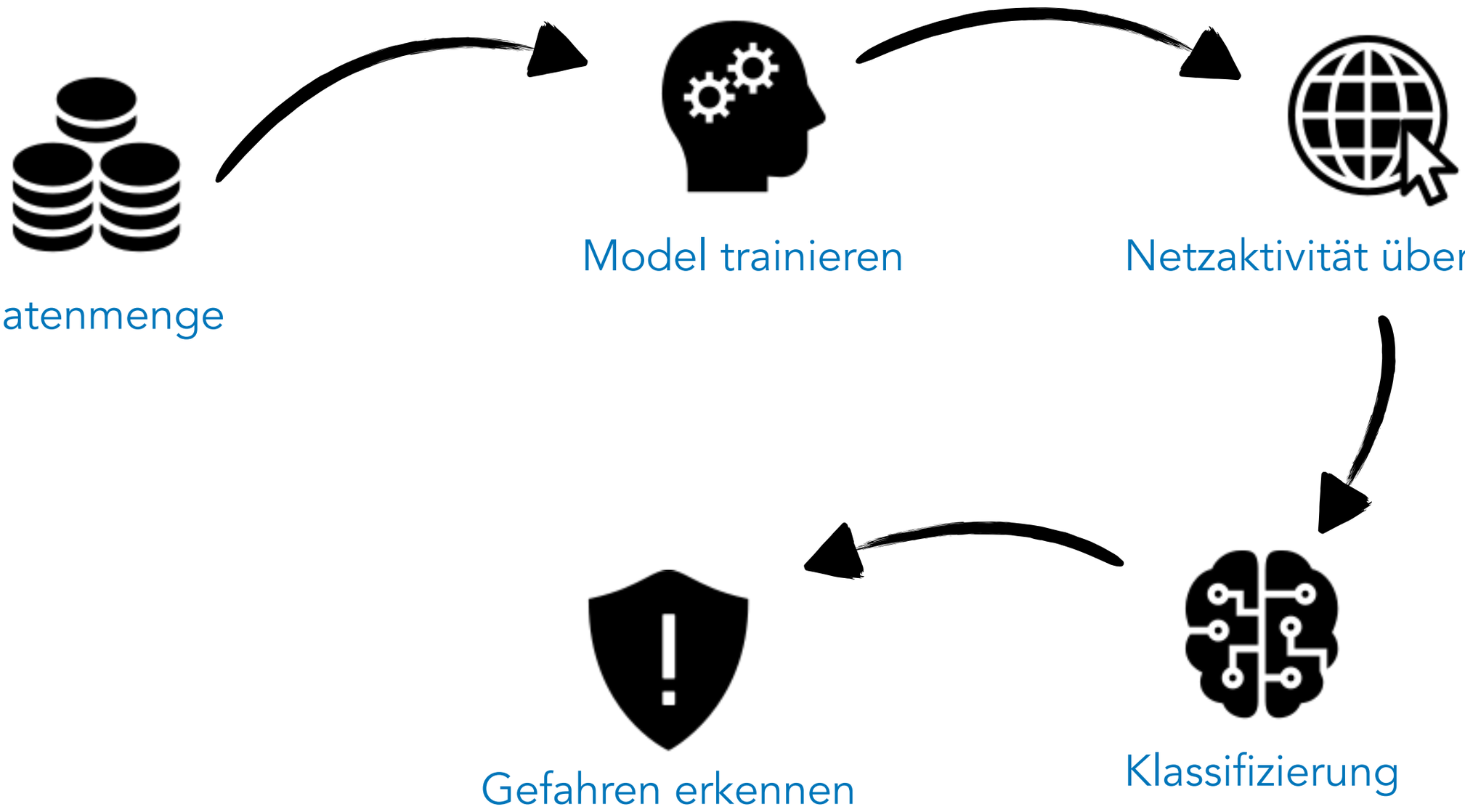


Netzaktivität überwachen

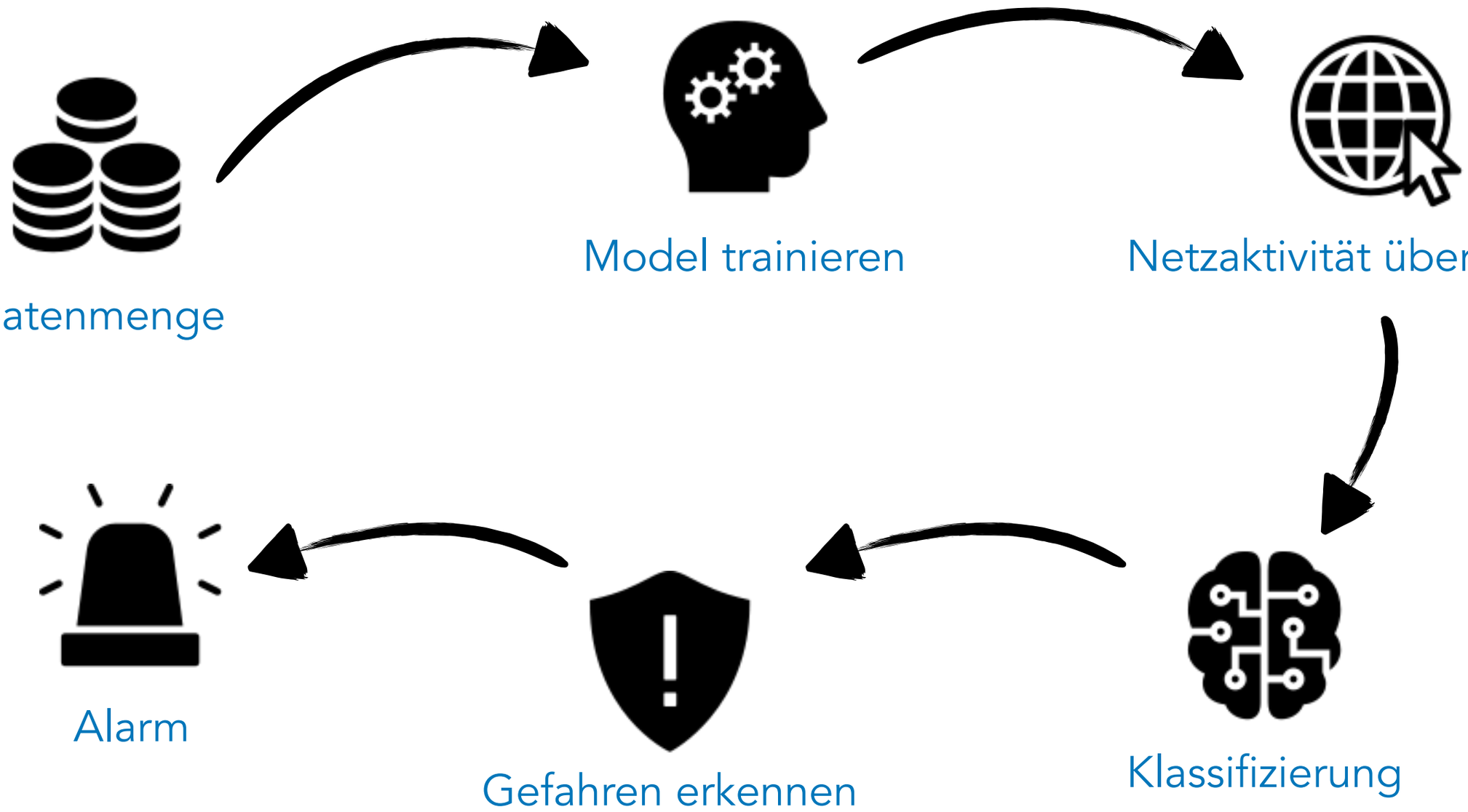


Klassifizierung

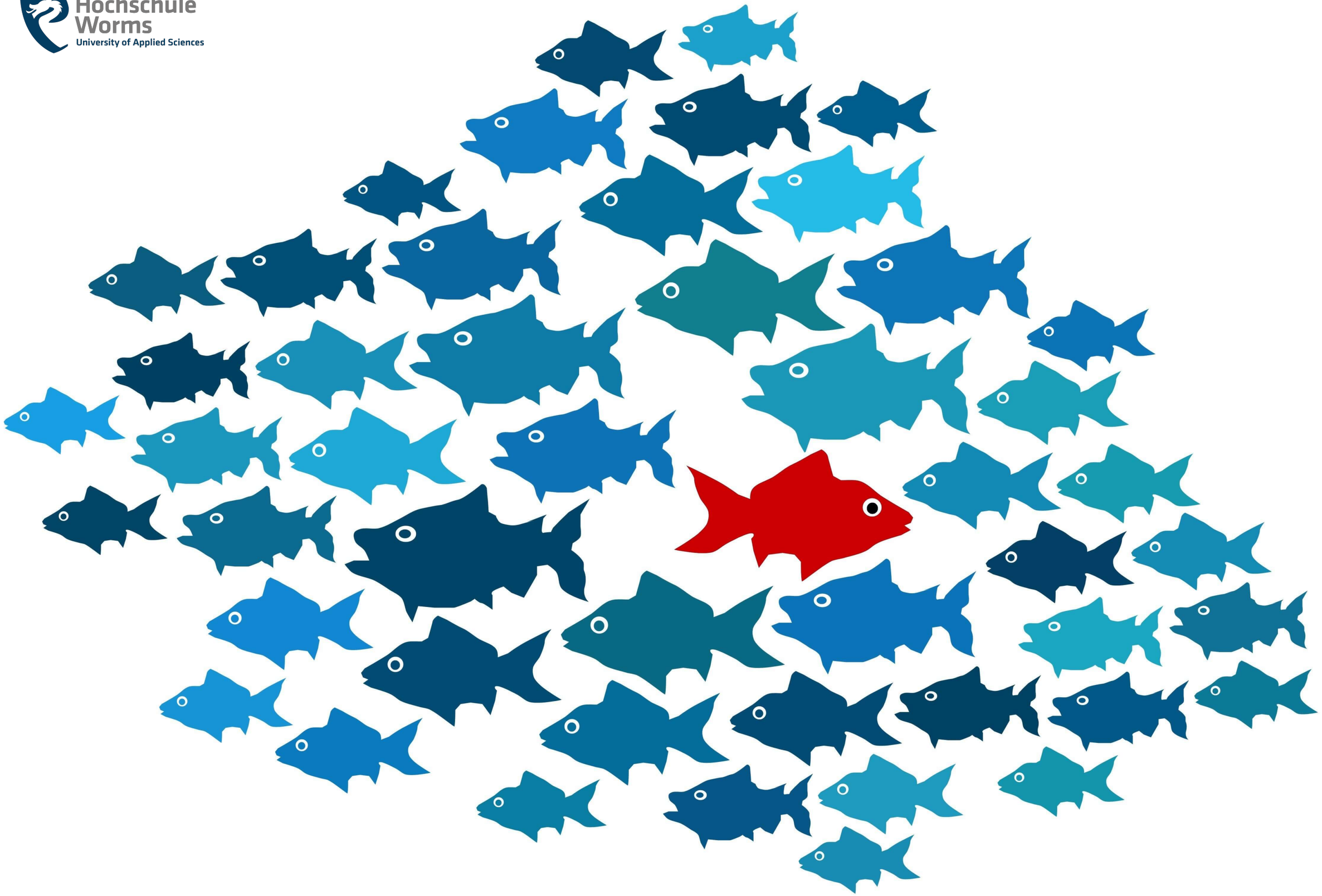
Anomaly-based IDS



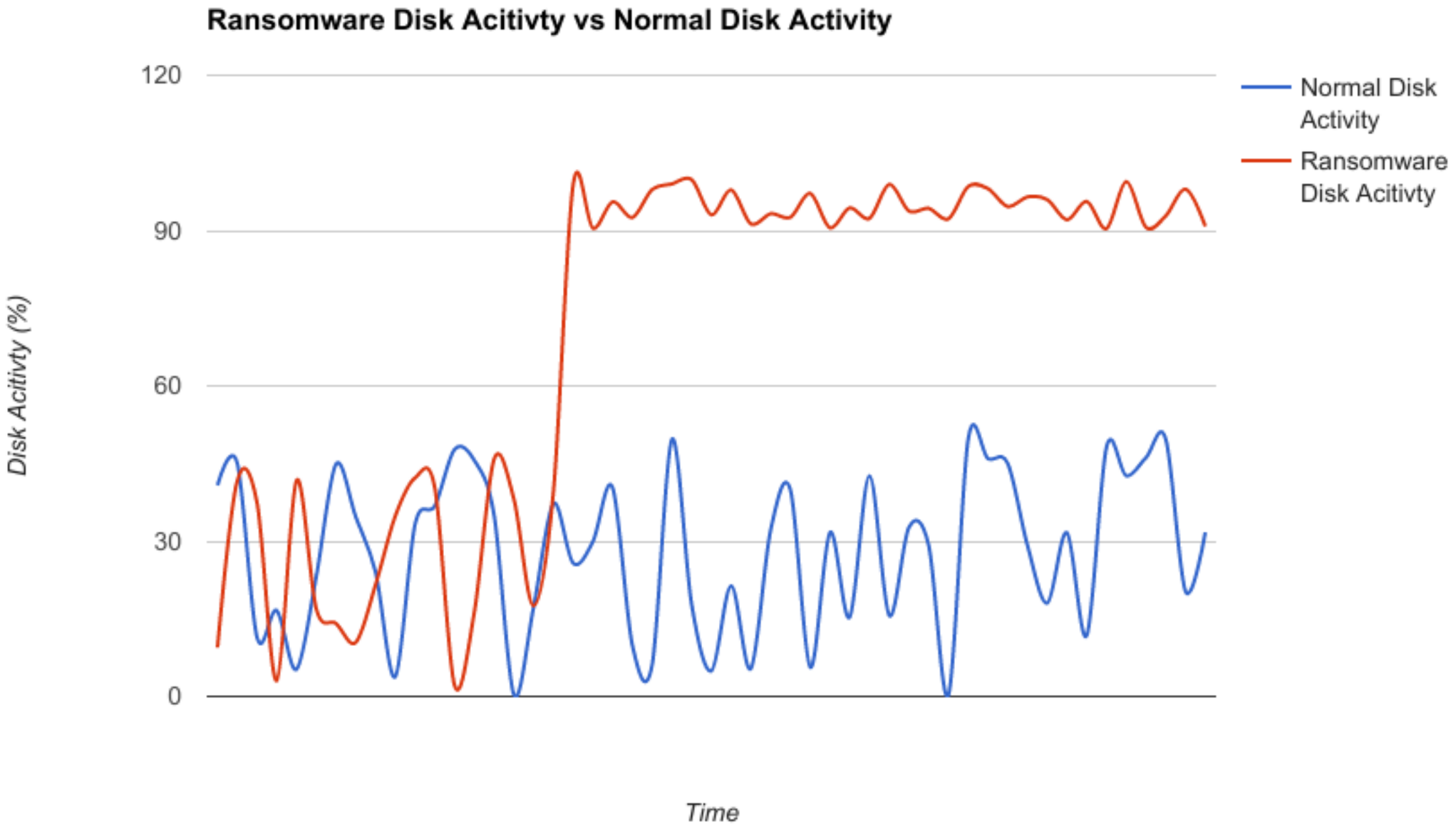
Anomaly-based IDS



Hochschule Worms
University of Applied Sciences



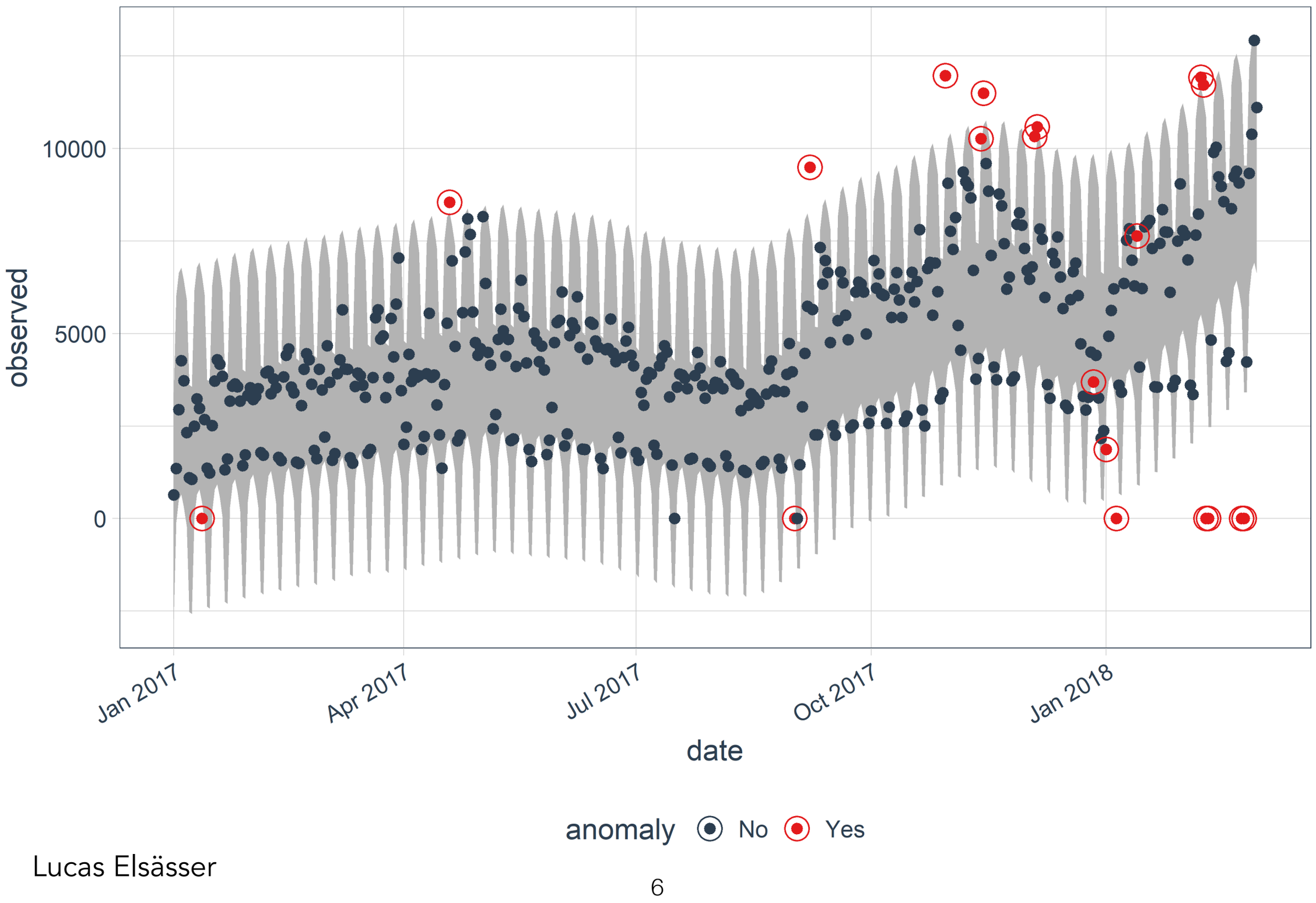
Lucas Elsässer


Ransomware Disk Acitivty vs Normal Disk Activity
120
90
60
30
0
Disk Acitivty (%)
Time
Normal Disk Activity
Ransomware Disk Acitivty

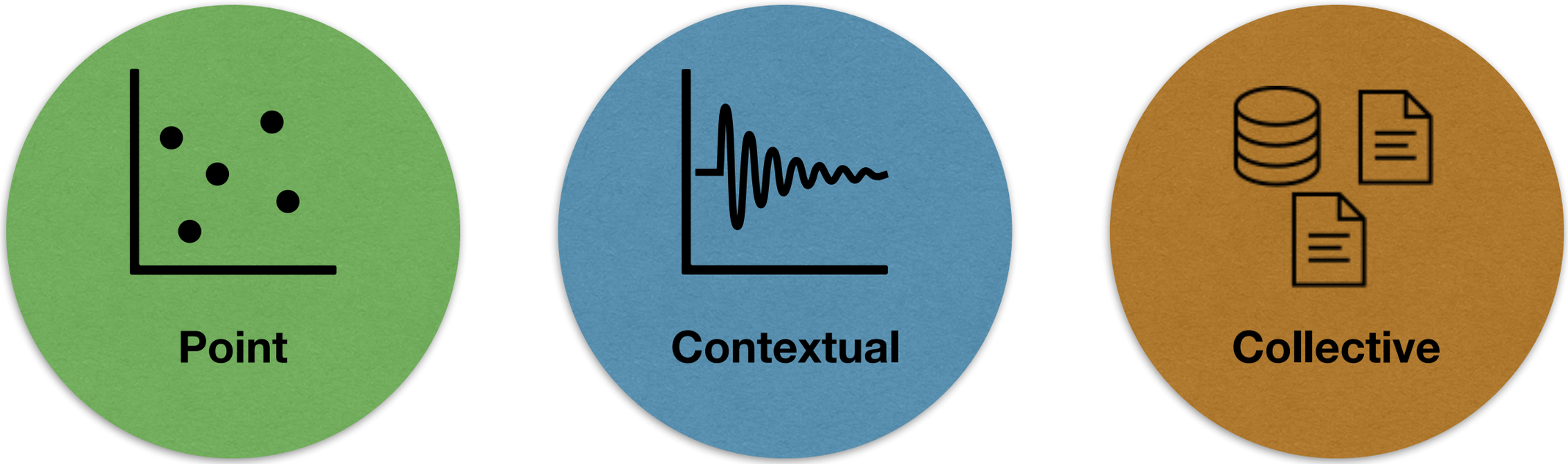
Hochschule Worms
University of Applied Sciences

Lubridate Anomalies

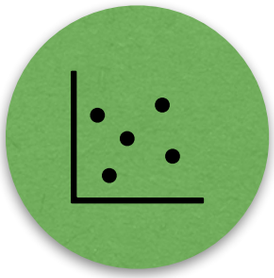
STL + IQR Methods

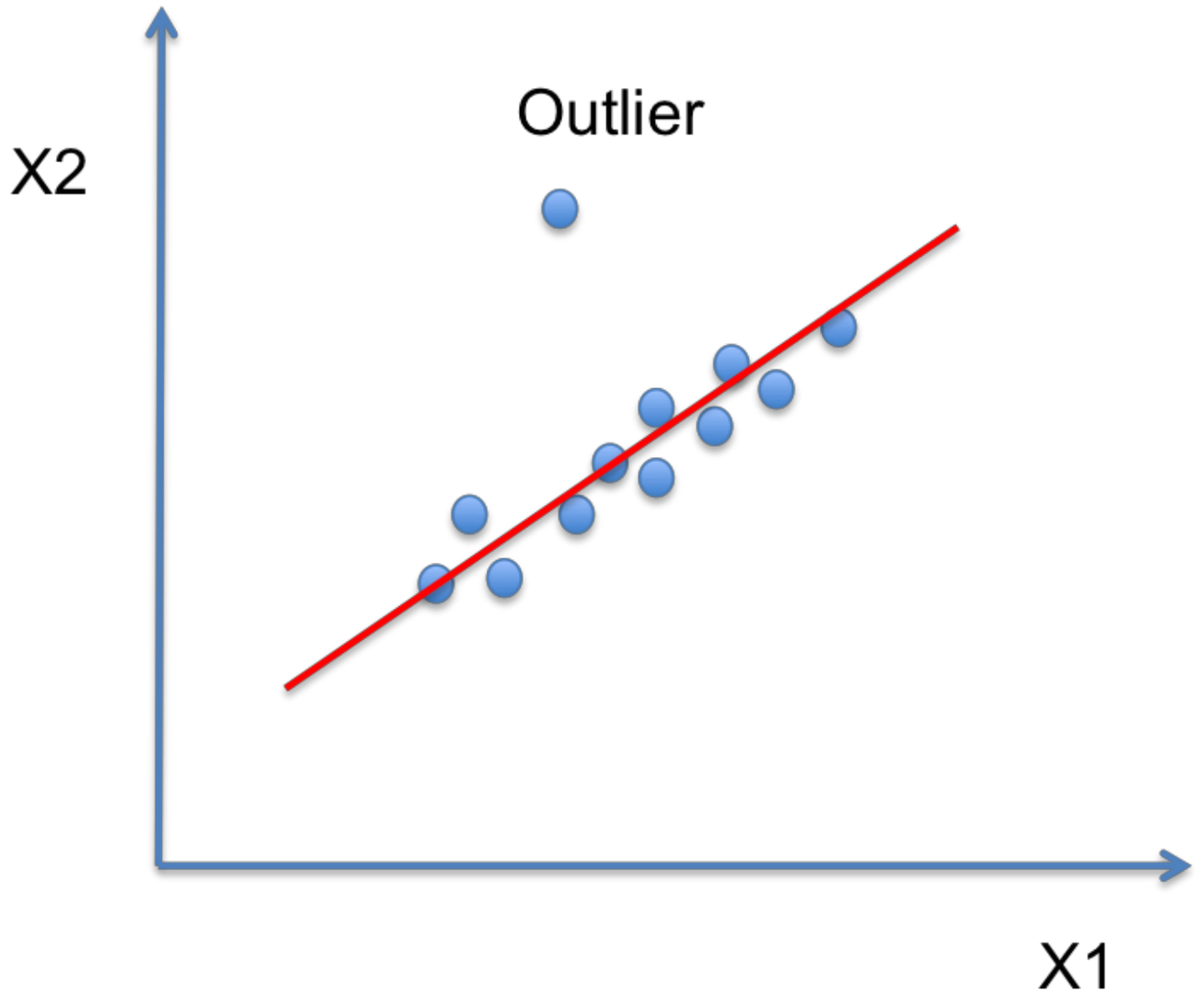


Anomalien

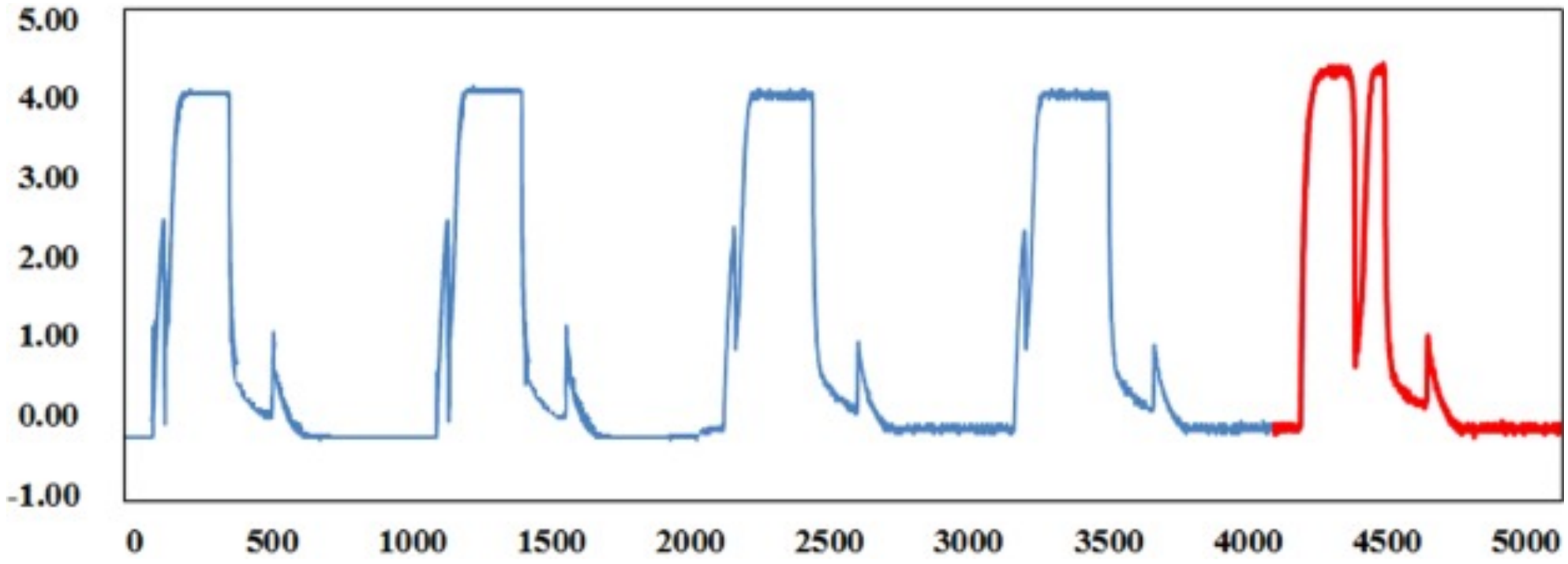


Point anomaly



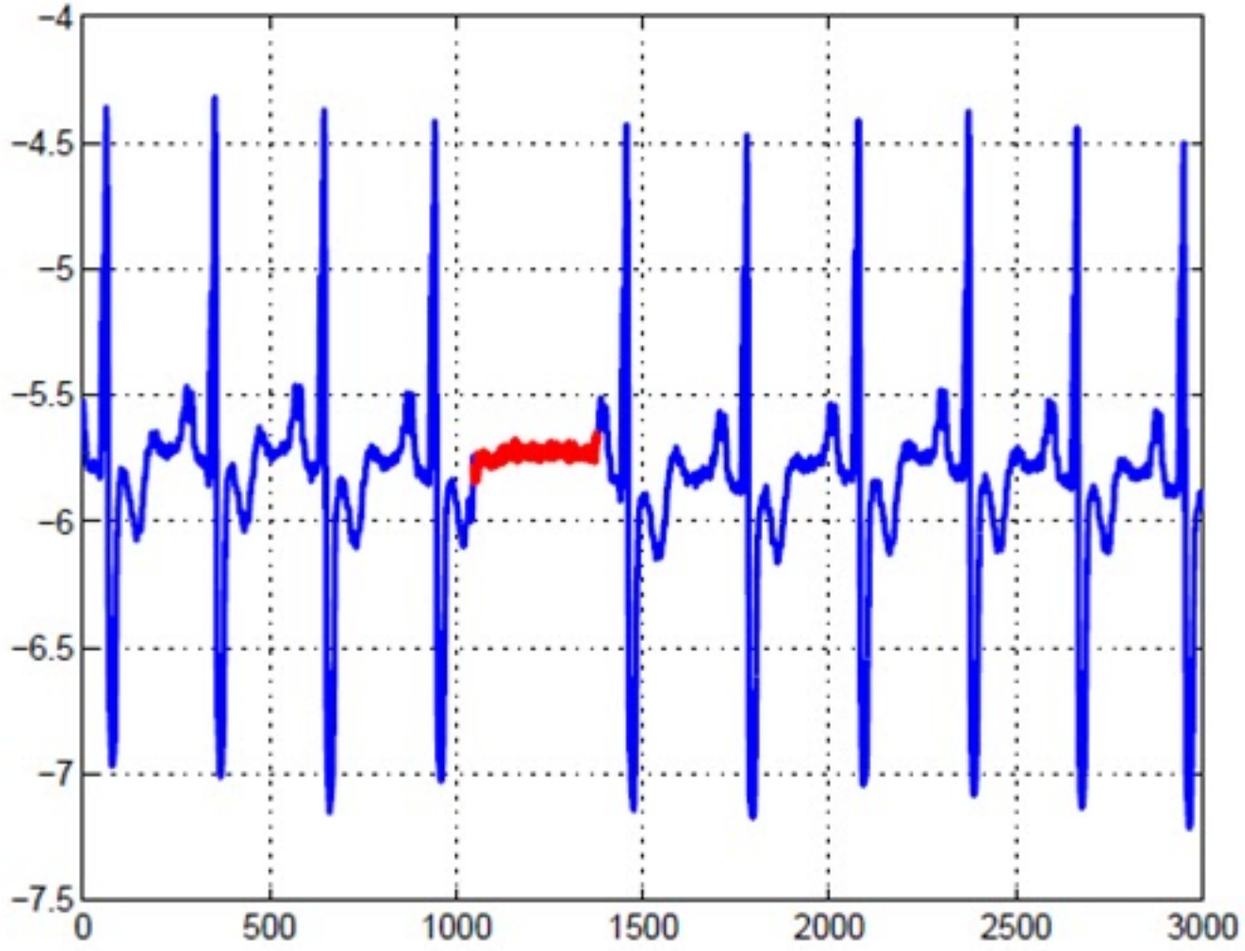


Contextual anomaly



Hochschule Worms
University of Applied Sciences

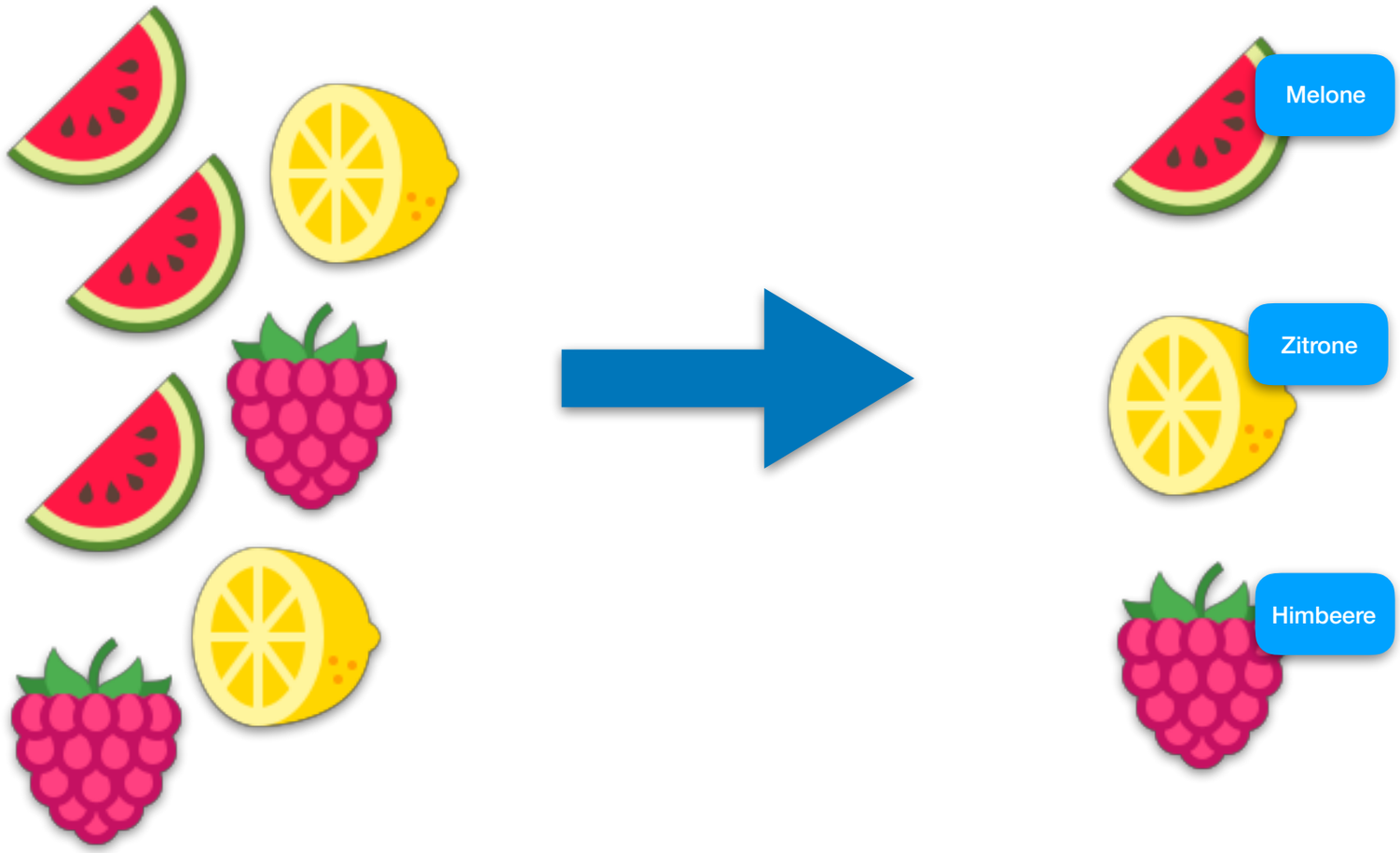
Collective anomaly



Hochschule Worms
University of Applied Sciences

Machine Learning

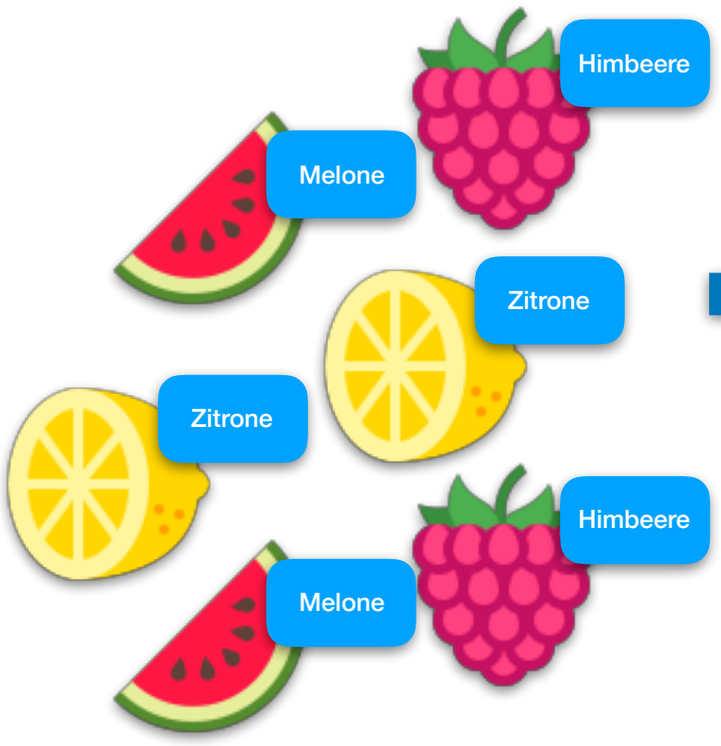
Supervised Learning



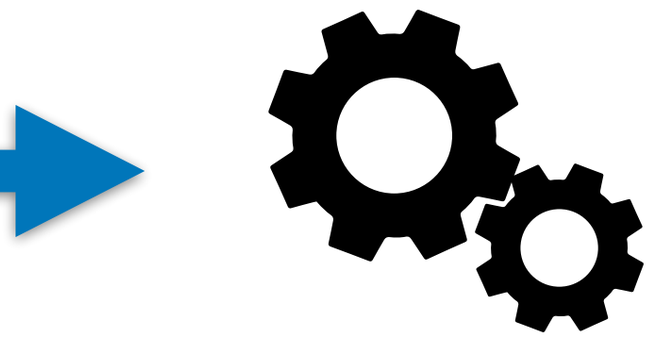
Datenmenge

Label

Supervised Learning



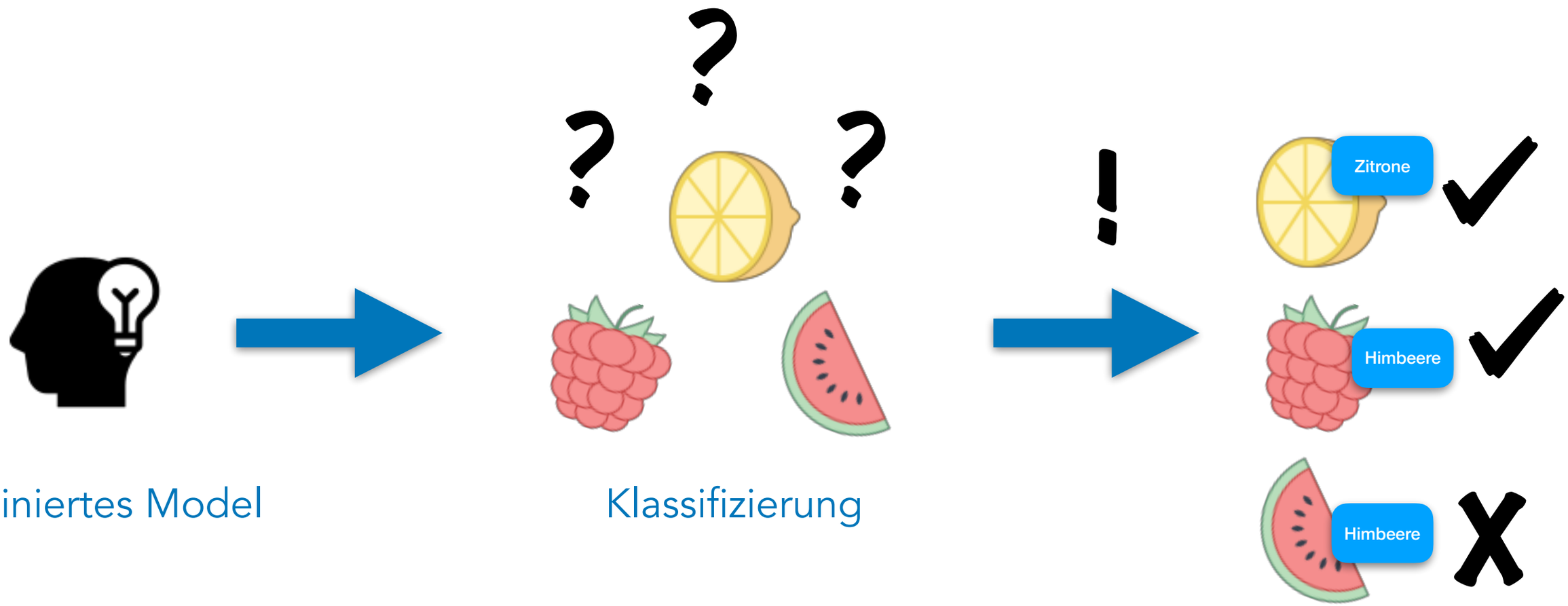
Datenmenge



Training / Lernvorgang

Trainiertes Model

Supervised Learning



Trainiertes Model

Klassifizierung

Evaluierung

Let’s see how this works!

Vergleich

Signature-based IDS	Anomaly-based IDS
nur bekannte Angriffe	soll neue Attacken erkennen
Erfordert Signatur Datenbank	Erfordert Trainingsdaten
Echtzeit-Pattern-Matching	Echtzeit-Klassifikation

Grafiken

- https://medium.com/@alhadpofali_5697/anomaly-and-outlier-detection-concepts-1f82498851a2
- https://www.datascience.com/blog/python-anomaly-detection
- https://stats.stackexchange.com/questions/323553/difference-between-contextual-anomaly-and-collective-anomaly
- https://ars.els-cdn.com/content/image/1-s2.0-S0957417416301191-gr2.jpg
- https://icons8.de/icons
- http://www.dataversity.net/machine-learning-next-decade-promises-pitfalls/

Papers

Rui Zhang, Shaoyan Zhang, Yang Lan, Jianmin Jiang. *Network Anomaly Detection Using One Class Support Vector Machine.* Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I IMECS 2008, 19-21 March, 2008, Hong Kong. https://bit.ly/2SRKuWG

Prajowal Manandhar, Zeyar Aung. *Towards Practical Anomaly-based Intrusion Detection by Outlier Mining on TCP Packets*. Institute Center for Smart and Sustainable Systems (iSmart) Masdar Institute of Science and Technology, Abu Dhabi, UAE. https://bit.ly/2Ex8Thi

V. Jyothsna, V. V. Rama Prasad. *A Review of Anomaly based IntrusionDetection Systems*. International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, September 2011. https://bit.ly/2S1UVac

Varun Chandola, Arindam Banerjee, Vipin Kumar. Anomaly Detection : A Survey. ACM Computing Surveys, September 2009. https://bit.ly/2SRQoXY

Robin Sommer, Vern Paxson. *Outside the Closed World: On Using Machine Learning For Network Intrusion Detection*. https://bit.ly/2NsYgxi

Stefan Axelsson. *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection*. https://bit.ly/1r27yTU

Hochschule Worms
University of Applied Sciences

VIELEN DANK!

Lucas Elsässer

Diskussion

Diskussion

- Muss der Trainingsvorgang an ein Unternehmen angepasst werden?

Diskussion

- Muss der Trainingsvorgang an ein Unternehmen angepasst werden?
- Hauptschwierigkeiten beim Training? Klassenverteilung?

Diskussion

- Muss der Trainingsvorgang an ein Unternehmen angepasst werden?
- Hauptschwierigkeiten beim Training? Klassenverteilung?
- Aktuelles Einsatzgebiet? Kombination mit Signature-based IDS?