AI in Cybersecurity

Tobias Oberrauch

Agenda

Agenda

- What is AI and ML?

Agenda

What is AI and ML?

What is Cybersecurity?

Agenda

- What is AI and ML?
- What is Cybersecurity?
- AI in Cybersecurity

Agenda

- What is AI and ML?
- What is Cybersecurity?
- AI in Cybersecurity
- Use case

Agenda

- What is AI and ML?
- What is Cybersecurity?
- AI in Cybersecurity
- Use case
- How to implement

Who am I?

Who am I?

15
years

Who am I?

15 years

Azure

Who am I?

15 years

Azure

AWS

Who am I?

15 years

Azure

AWS

AI

Who am I?

15 years | Azure | AWS | AI

CGI

Executive Consultant CGI

Who am I?

15 years | Azure | AWS | AI

CGI
Executive Consultant CGI

KI BUNDESVERBAND
German AI Association

What is AI?

What is AI?

Automation of intelligent behavior and machine learning.

What is AI?

Automation of intelligent behavior and machine learning.

What is AI?

Automation of intelligent behavior and machine learning.

Strong and weak AI

Weak AI

Strong AI

Strong and weak AI

Weak AI

- Application specific & task limited

Strong AI

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers

Strong AI

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding

Strong AI

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding
- Knowledge does not transfer to other domains or tasks

Strong AI

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding
- Knowledge does not transfer to other domains or tasks
- Today

Strong AI

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding
- Knowledge does not transfer to other domains or tasks
- Today

Strong AI

- Perform general (human) intelligenz action

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding
- Knowledge does not transfer to other domains or tasks
- Today

Strong AI

- Perform general (human) intelligenz action
- Self-learns and reasons with its operating environment

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding
- Knowledge does not transfer to other domains or tasks
- Today

Strong AI

- Perform general (human) intelligenz action
- Self-learns and reasons with its operating environment
- Full range of human cognitive abilities

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding
- Knowledge does not transfer to other domains or tasks
- Today

Strong AI

- Perform general (human) intelligenz action
- Self-learns and reasons with its operating environment
- Full range of human cognitive abilities
- Leverages knowledge transfer to new domains and tasks

Strong and weak AI

Weak AI

- Application specific & task limited
- Fixed domain models provided by programmers
- Reflexive tasks with no understanding
- Knowledge does not transfer to other domains or tasks
- Today

Strong AI

- Perform general (human) intelligenz action
- Self-learns and reasons with its operating environment
- Full range of human cognitive abilities
- Leverages knowledge transfer to new domains and tasks
- Future

What is machine learning?

What is machine learning?

Supervised learning

What is machine learning?

Supervised learning

- Algorithms: Classification and regression

What is machine learning?

Supervised learning

- Algorithms: Classification and regression
- Usage: Spam filter, Weather forecast, price prediction...

What is machine learning?

Supervised learning

- Algorithms: Classification and regression
- Usage: Spam filter, Weather forecast, price prediction...
- How it works: Use of data marked with labels

What is machine learning?

Supervised learning

- Algorithms: Classification and regression
- Usage: Spam filter, Weather forecast, price prediction...
- How it works: Use of data marked with labels

Unsupervised learning

What is machine learning?

Supervised learning

- Algorithms: Classification and regression
- Usage: Spam filter, Weather forecast, price prediction...
- How it works: Use of data marked with labels

Unsupervised learning

- Algorithms: Clustering, Association and Dimensionality reduction

What is machine learning?

Supervised learning

- Algorithms: Classification and regression
- Usage: Spam filter, Weather forecast, price prediction...
- How it works: Use of data marked with labels

Unsupervised learning

- Algorithms: Clustering, Association and Dimensionality reduction
- Usage: Anomaly detection, Analyse medical images, Basket analysis...

What is machine learning?

Supervised learning

- Algorithms: Classification and regression
- Usage: Spam filter, Weather forecast, price prediction...
- How it works: Use of data marked with labels

Unsupervised learning

- Algorithms: Clustering, Association and Dimensionality reduction
- Usage: Anomaly detection, Analyse medical images, Basket analysis...
- How it works: Detection of hidden patterns without external influences

What is machine learning?

Supervised learning

- Algorithms: Classification and regression
- Usage: Spam filter, Weather forecast, price prediction...
- How it works: Use of data marked with labels

Unsupervised learning

- Algorithms: Clustering, Association and Dimensionality reduction
- Usage: Anomaly detection, Analyse medical images, Basket analysis...
- How it works: Detection of hidden patterns without external influences

Reinforcement learning

What is cybersecurity?

What is cybersecurity?

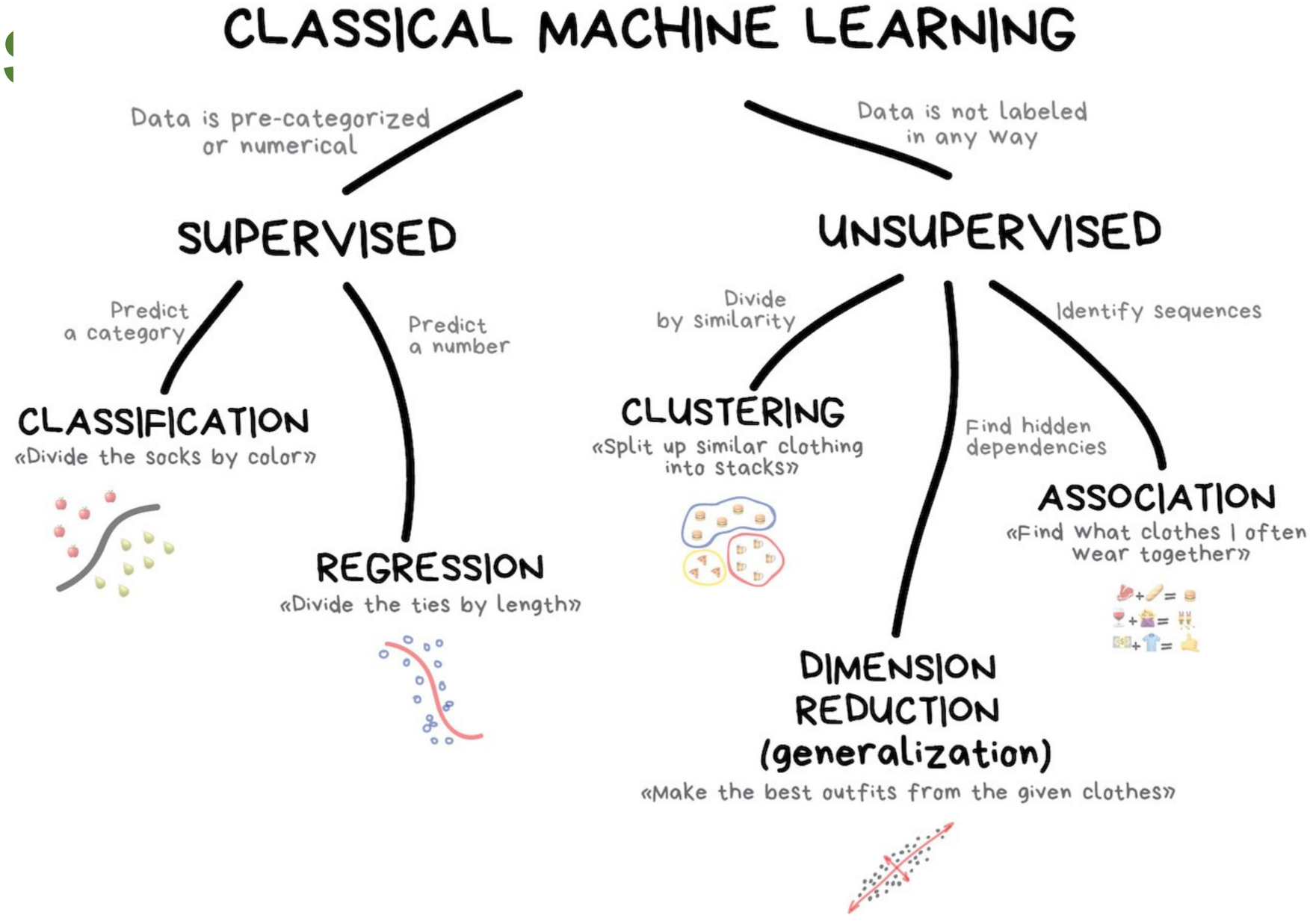
AI in Cybersecurity

Start with first use case

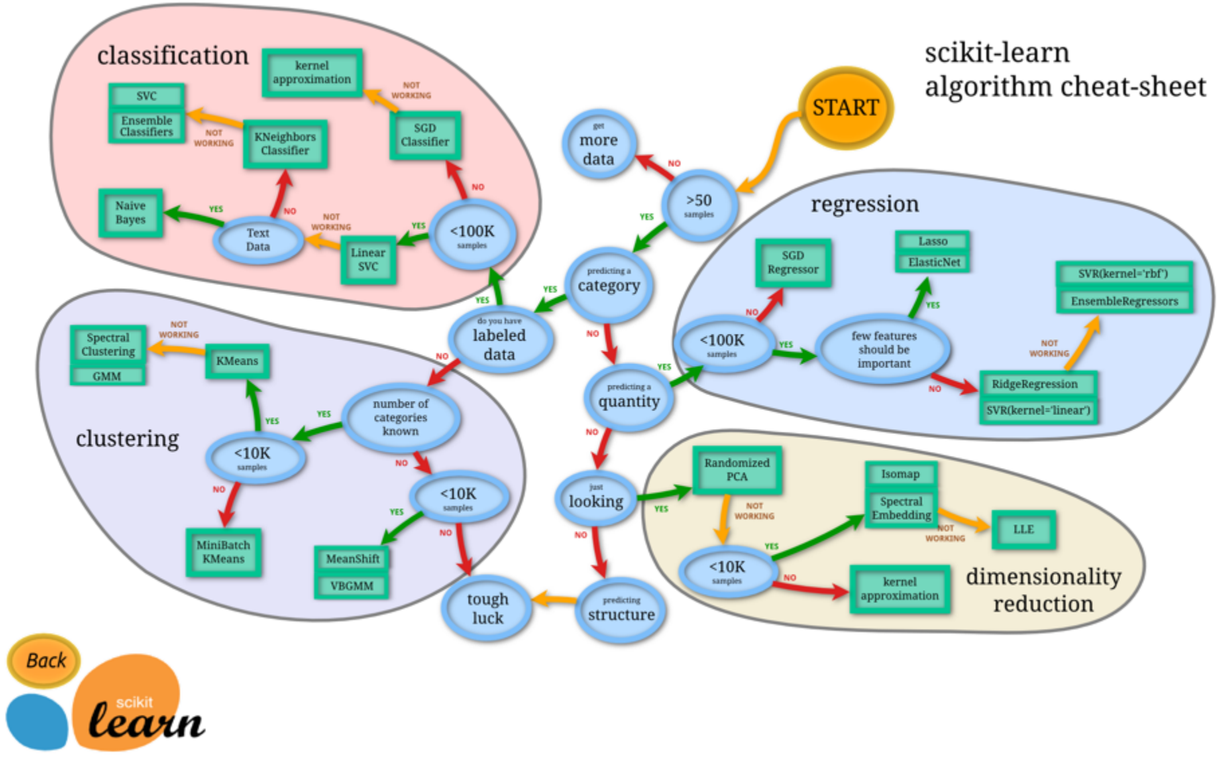
What is cybersecurity?

Find use cases

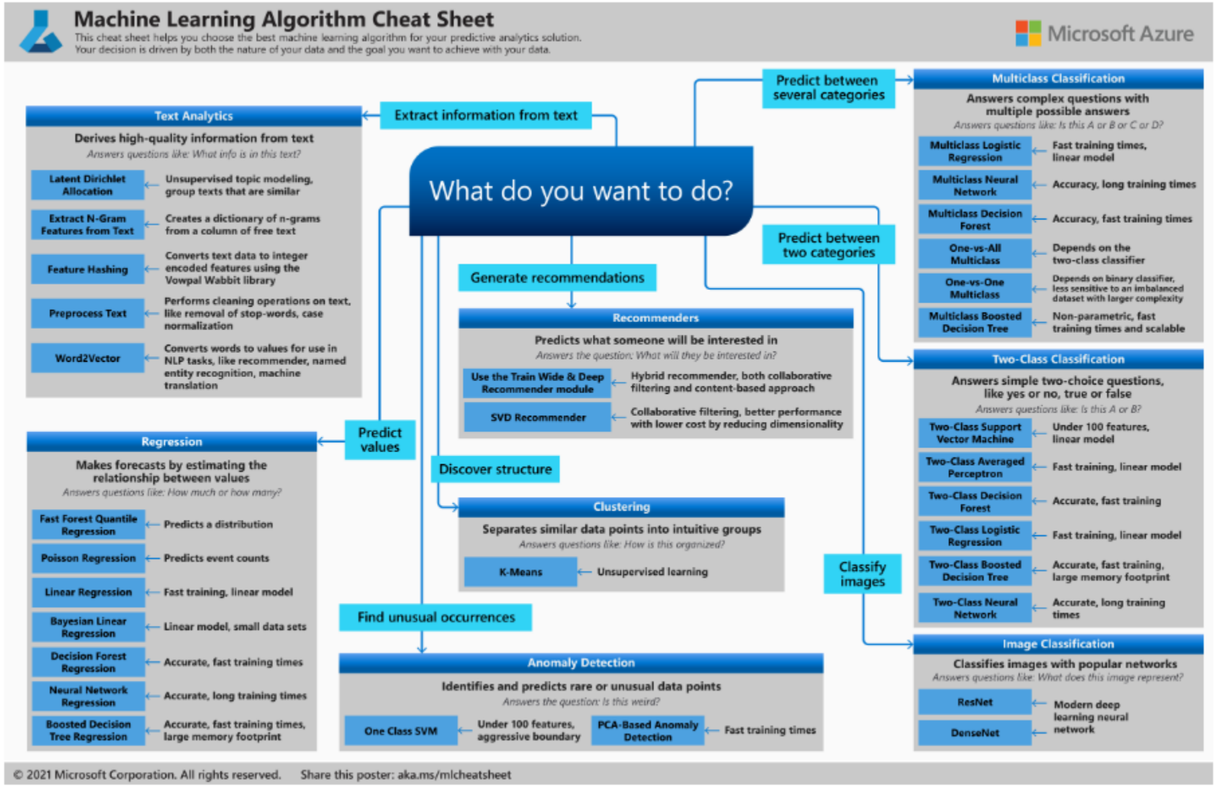
What is


CLASSICAL MACHINE LEARNING
Data is pre-categorized or numerical
Data is not labeled in any way
SUPERVISED
UNSUPERVISED
Predict a category
Predict a number
Divide by similarity
Identify sequences
CLASSIFICATION
«Divide the socks by color»
REGRESSION
«Divide the ties by length»
CLUSTERING
«Split up similar clothing into stacks»
Find hidden dependencies
ASSOCIATION
«Find what clothes I often wear together»
DIMENSION REDUCTION (generalization)
«Make the best outfits from the given clothes»

What is cybersecurity?



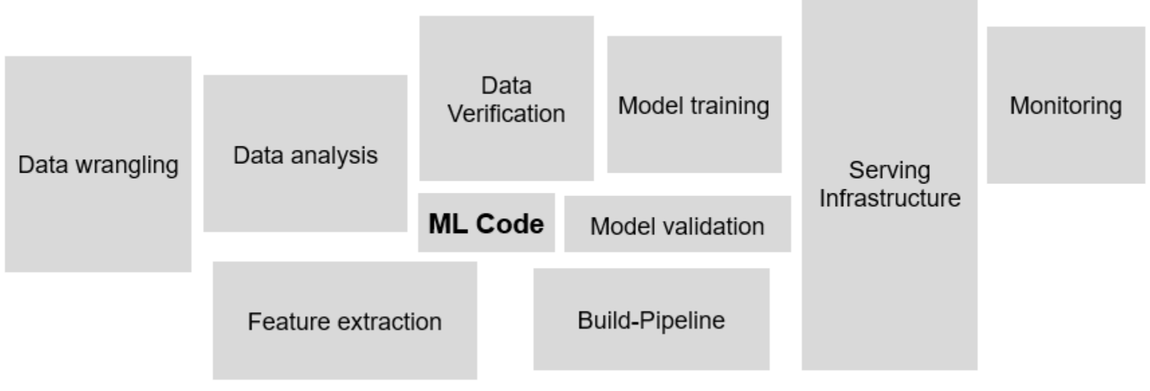
What is cybersecurity?



What is cybersecurity?

Implement

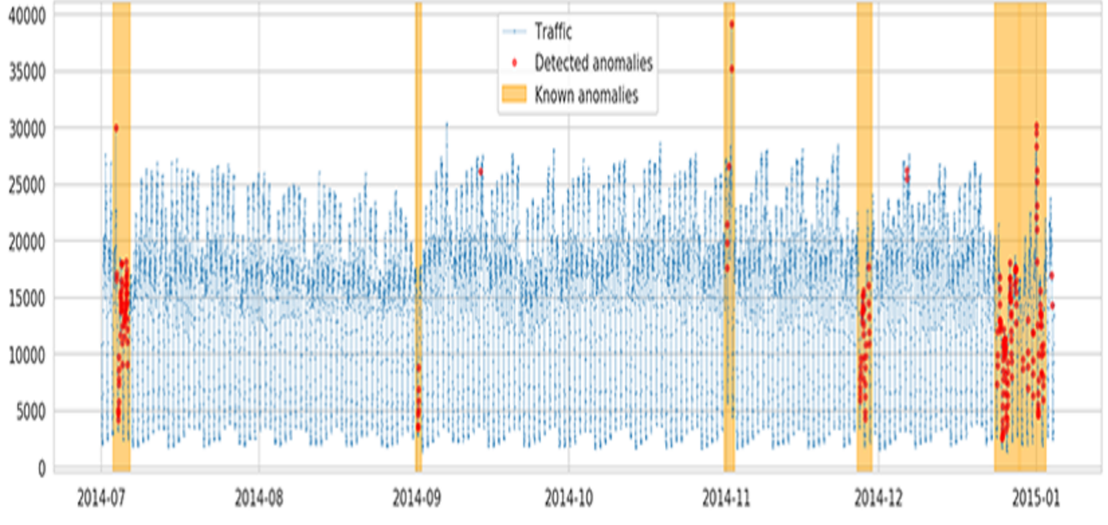
There is more than just ML code



What is cybersecurity?

Use case

Anomaly Detection



What is cybersecurity?

Summary

What is cybersecurity?

Summary

Make or buy

What is cybersecurity?

Summary

Make or buy

Do you really need ai?

What is cybersecurity?

Summary

Make or buy

Do you really need ai?

Choose one use case