Cybersecurity, AI and Honeytokens

Ordina Belgium

Emmanouil Perselis

Why?

- Challenges
  - Alert fatigue
  - Increased workload
  - Human error

- Goals
  - Increased alert fidelity
  - Lower amount of alerts
  - Increased analysis quality

Honeytokens

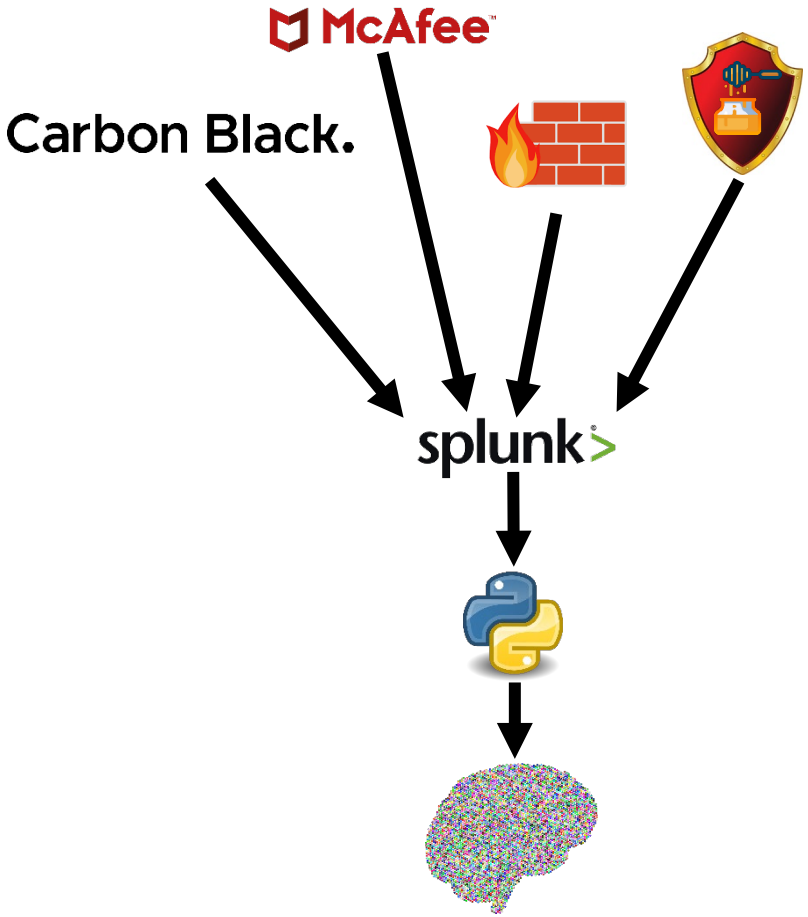
- Digital entities that trigger alerts when accessed
  - DNS records
  - URIs
  - Documents
  - Accounts
  - Database records
  - Registry keys

What & How?

- Alert classification
  - Combined multiple data sources
  - Makes use of business context
  - Adds honeytokens into the equation (increases true positive rate)
  - Multidisciplinary correlation engine

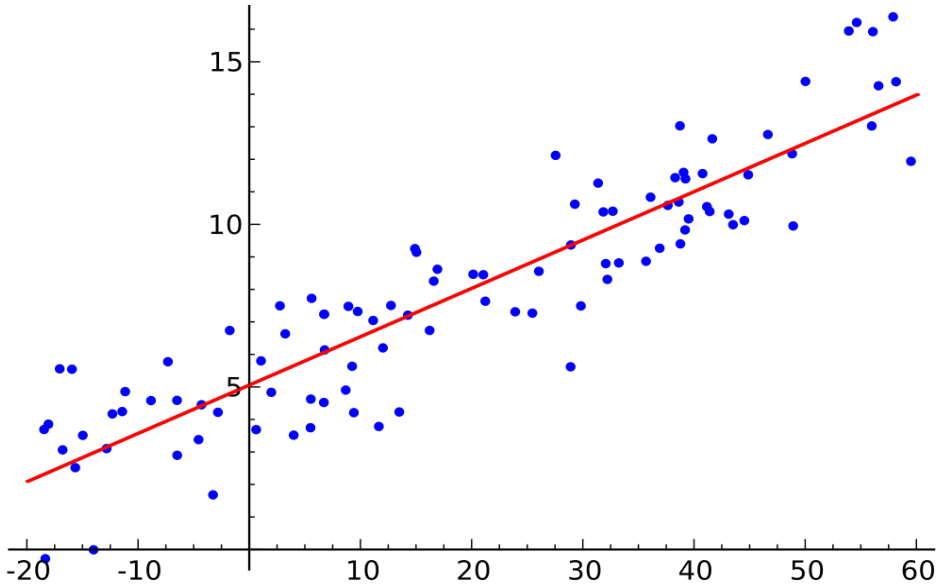
What & How?

- Used tools
  - Web gateway
  - AV solution
  - EDR solution
  - Splunk
  - Python & AI
  - Honeytokens



What & How?

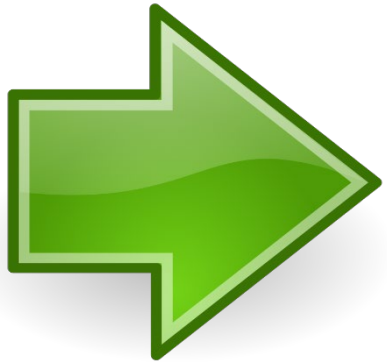
- Used model
  - Logistic Regression
    - High accuracy
    - Simple data presentation
    - Only 2 categories
    - Comes with a performance price



- Other models tried
  - KNN
    - Was slow
    - We have many outliers
    - Many missing values
  - Naïve Bayes
    - Low quality predictions
    - Was faster though

Status & Looking forward

- Research phase
- Good results for the time being
- Checking applicability
- Checking efficacy
- Solving problems on integration of business context
- Go in acceptance in Q3 2020 – Q4 2020



Lessons learned

- Certain added value
- Given that there are only 2 classes, classification is efficient
- Manual triage is still necessary
- Most difficult part is adding (business) context to data
- Model training & fitting is resource intensive and has to be done outside office hours