AI – An opportunity for the EU cyber-crisis management

ML-BASED ANOMALY DETECTION IN INDUSTRIAL ENVIRONMENTS

04/06/2019

S2 GRUPO

- S2 Grupo
- Industrial and critical environments
- Anomaly detection process
- Water treatment plant
- IHoney
- Conclusions and next steps
- Other research lines: LM3

S2 GRUPO

More than 15 years of experience in cybersecurity

With offices in Spain, Belgium, Portugal, Colombia and Mexico and operations in more than **15 countries**

Over 300 Cybersecurity experts

50 R&D+i projects with more than 15% of our turnover invested per year

Security solutions:
- SOC management
- APT detection
- ICS CyberSecurity

Tools designed with **CCN-CERT**

S2 GRUPO CERT: 4 SOCs operating from Valencia, Madrid, Bogota and México

- TRUSTED
- FIRST

Specialized SOC:

- Industry 4.0
- Healthcare

Consulting Services:
- Incident Response, Forensic
- Security audits & Red team
- GRC
- Awareness programs

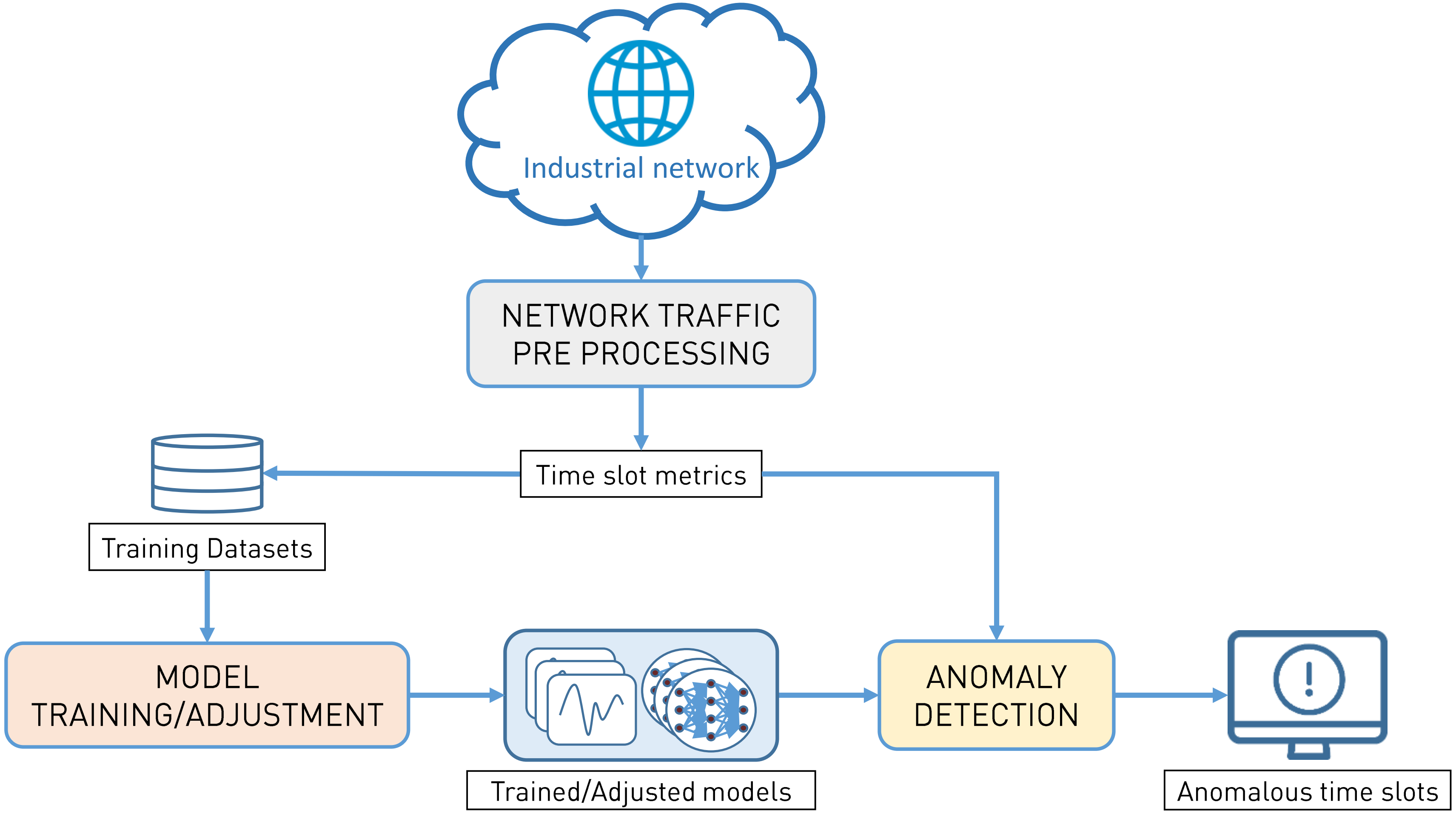
More than 9 certifications

INDUSTRIAL AND CRITICAL ENVIRONMENTS

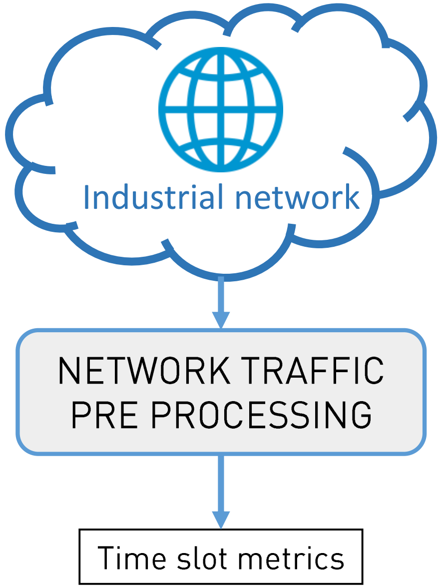
- **Longer life cycle than other ICT**
  - Presence of legacy technology
  - Lack of proper cybersecurity support
- **Intervention and updating issues**
  - Higher vulnerabilities presence
  - Larger response times
- **Lack of personnel with specific training in cybersecurity**

- **Traditional techniques**
  - Passive Vulnerability Scanning
  - Intrusion Detection System
  - Known attack signatures
- **Anomaly detection (Machine Learning)**
  - Clustering
  - Autoregression
  - Neural networks

ANOMALY DETECTION PROCESS



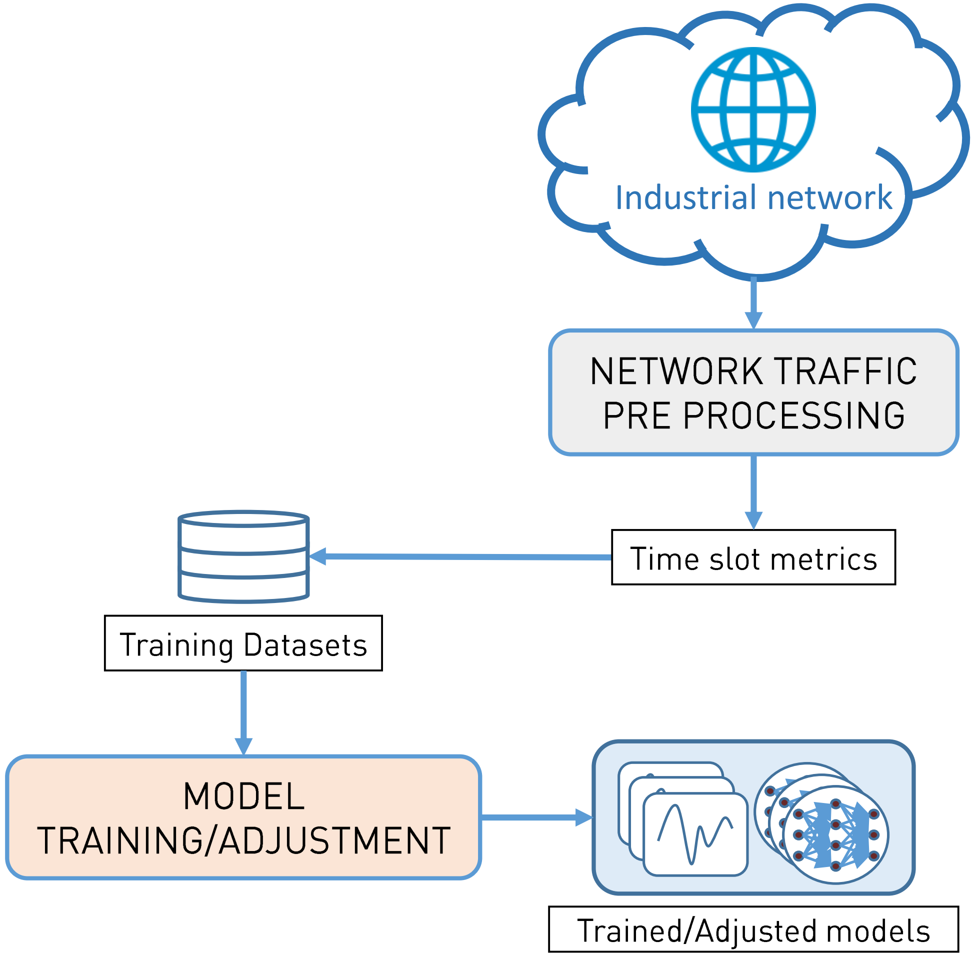
ANOMALY DETECTION PROCESS



PRE PROCESSING PHASE

- ICS protocols dissection
- Time slot aggregation
- Traditional metrics:
  Bytes
  Packets
  ...
- ML-Based metrics:
  Clustering
  Neural networks
  ...

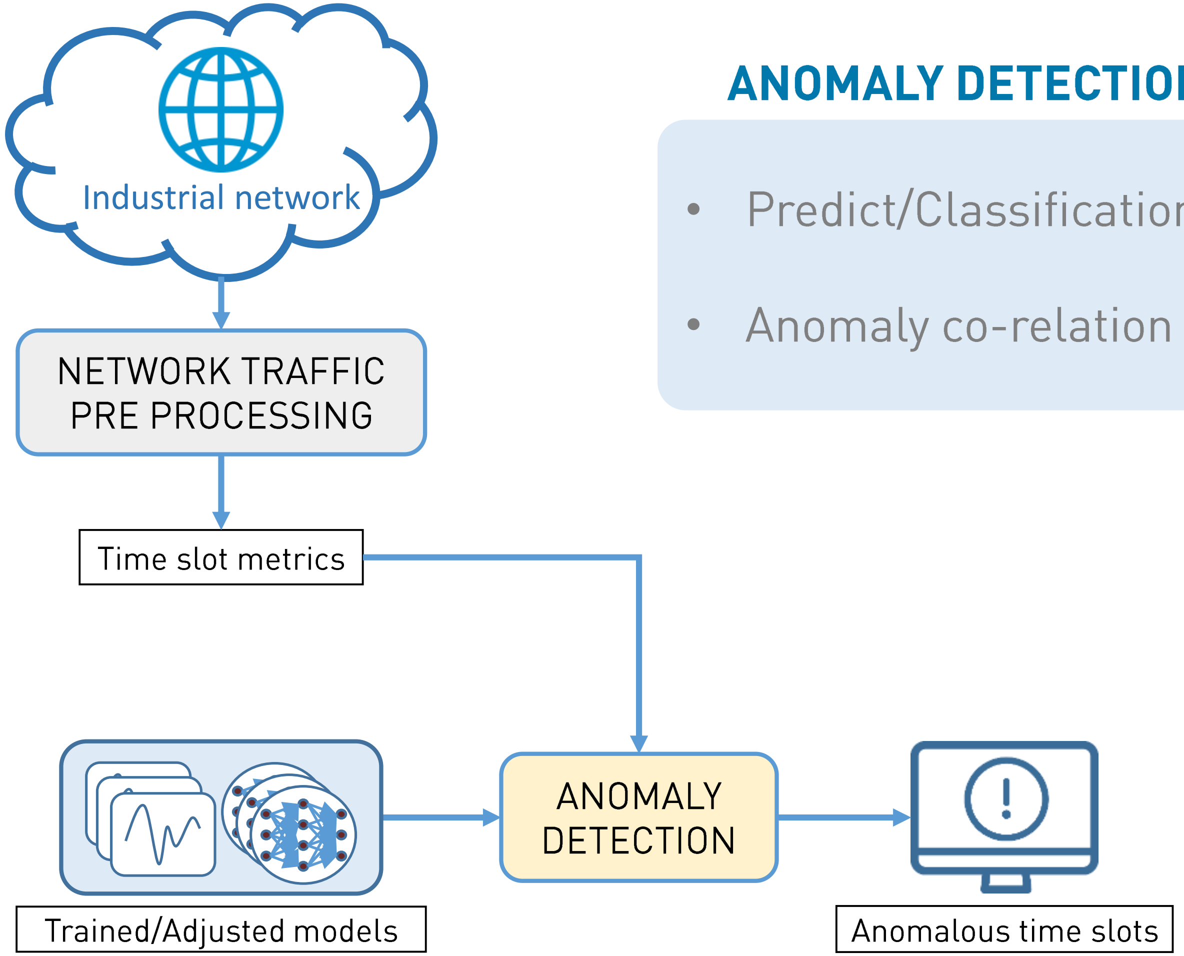
ANOMALY DETECTION PROCESS



TRAINING PHASE

- Different models for each metric
- Clustering analysis
- Time series analysis
  Regression
  Neural networks

ANOMALY DETECTION PROCESS



ANOMALY DETECTION PHASE

- Predict/Classification
- Anomaly co-relation

WATER TREATMENT PLANT

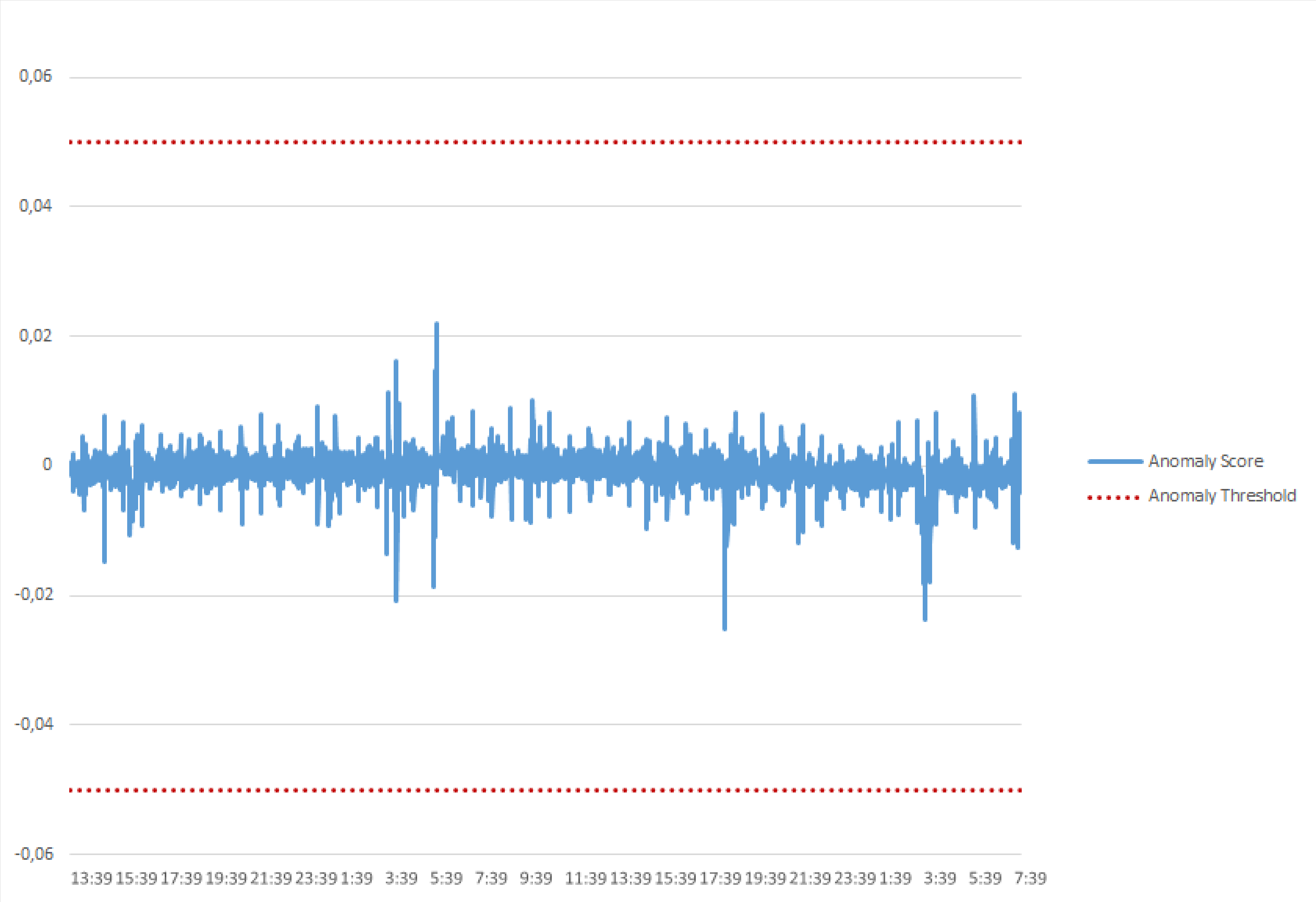
- **Production environment:**
  - Around 30 hosts in the network
  - Near 1/2 Tb/day traffic

WATER TREATMENT PLANT

NB. OF PACKETS (5 min): OBSERVED vs. PREDICTED

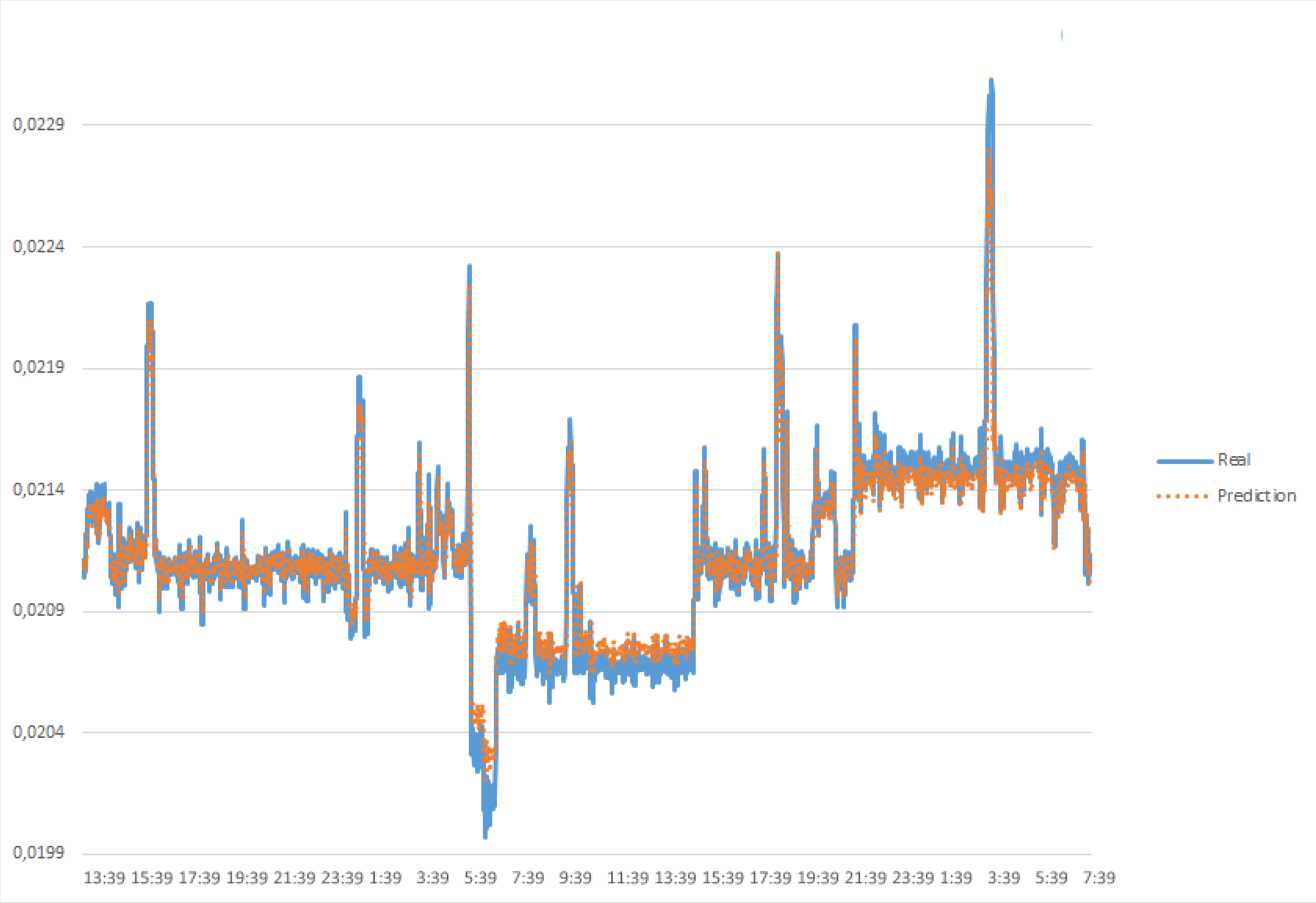
NB. OF PACKETS (5 min): ANOMALY SCORE

WATER TREATMENT PLANT



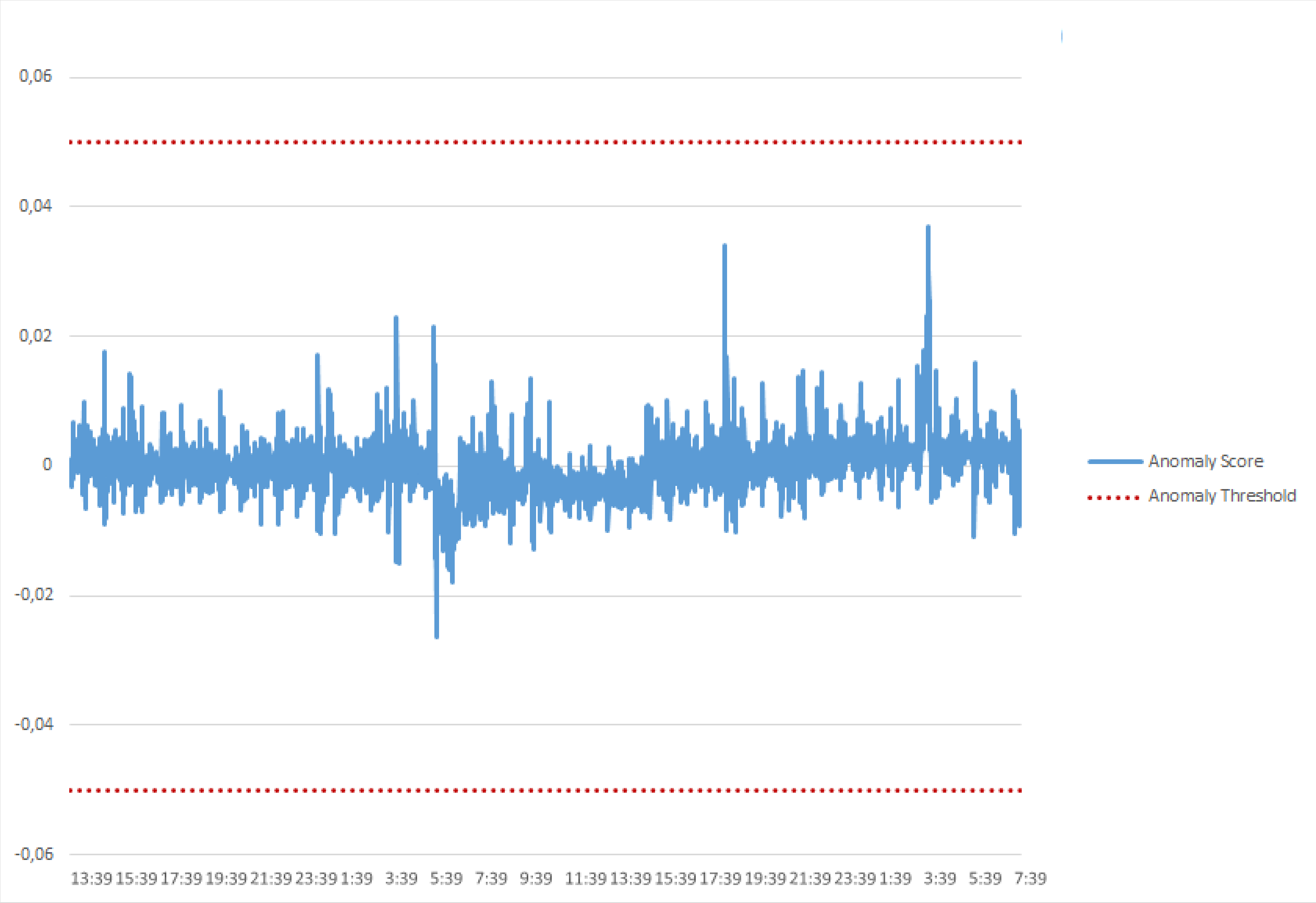
AVG. INTER ARRIVAL TIME (5 min): OBSERVED vs. PREDICTED

WATER TREATMENT PLANT



AVG. INTER ARRIVAL TIME (5 min): ANOMALY SCORE

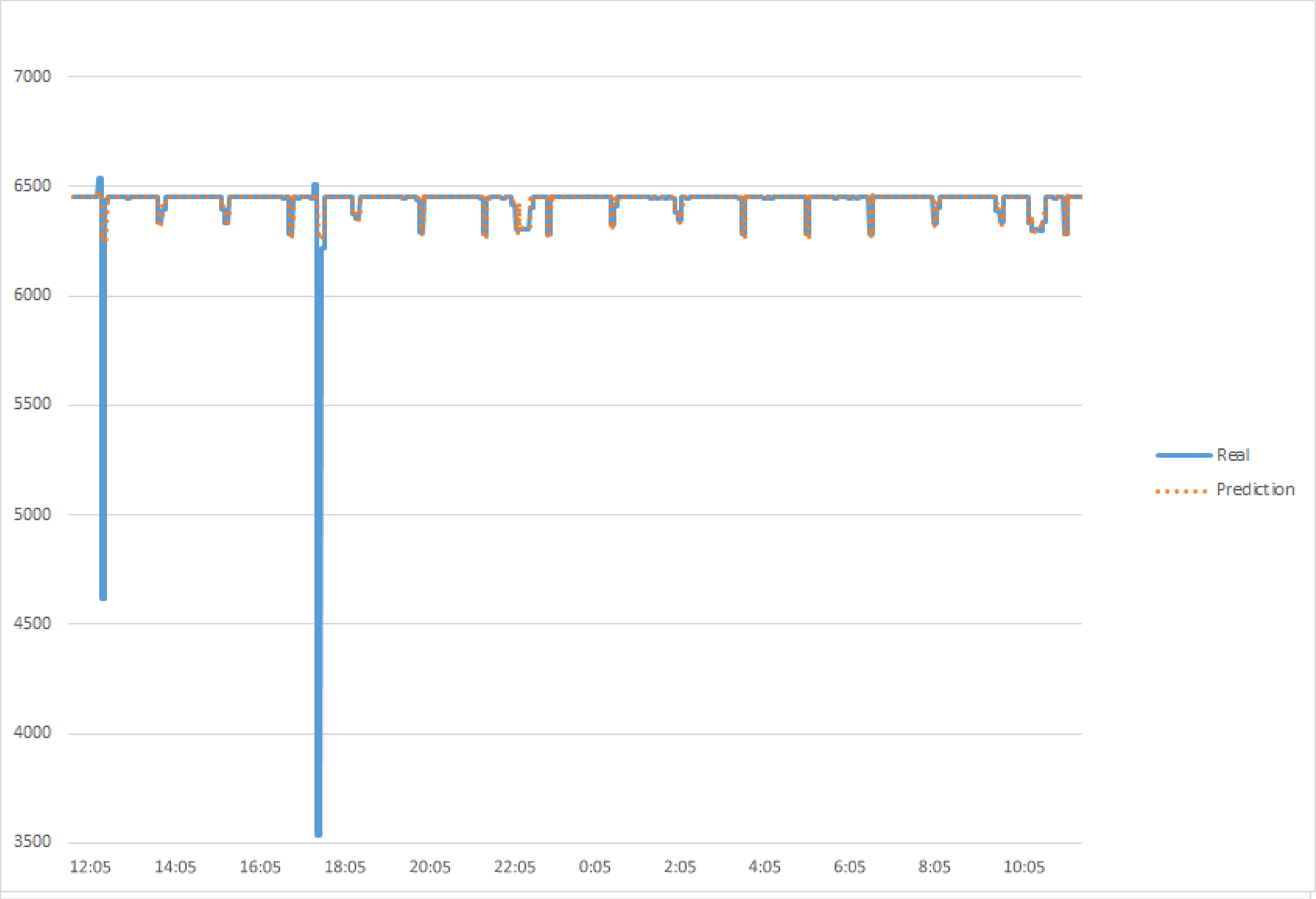
WATER TREATMENT PLANT



- **Water treatment plant honeypot**
  - 4 hosts in the network
  - Near 1Gb/day traffic
- **Realistic operation**
- **Experiments with real attacks**
- **More information on IHONEY**
  - https://s2grupo.es/en/ihoney_en/

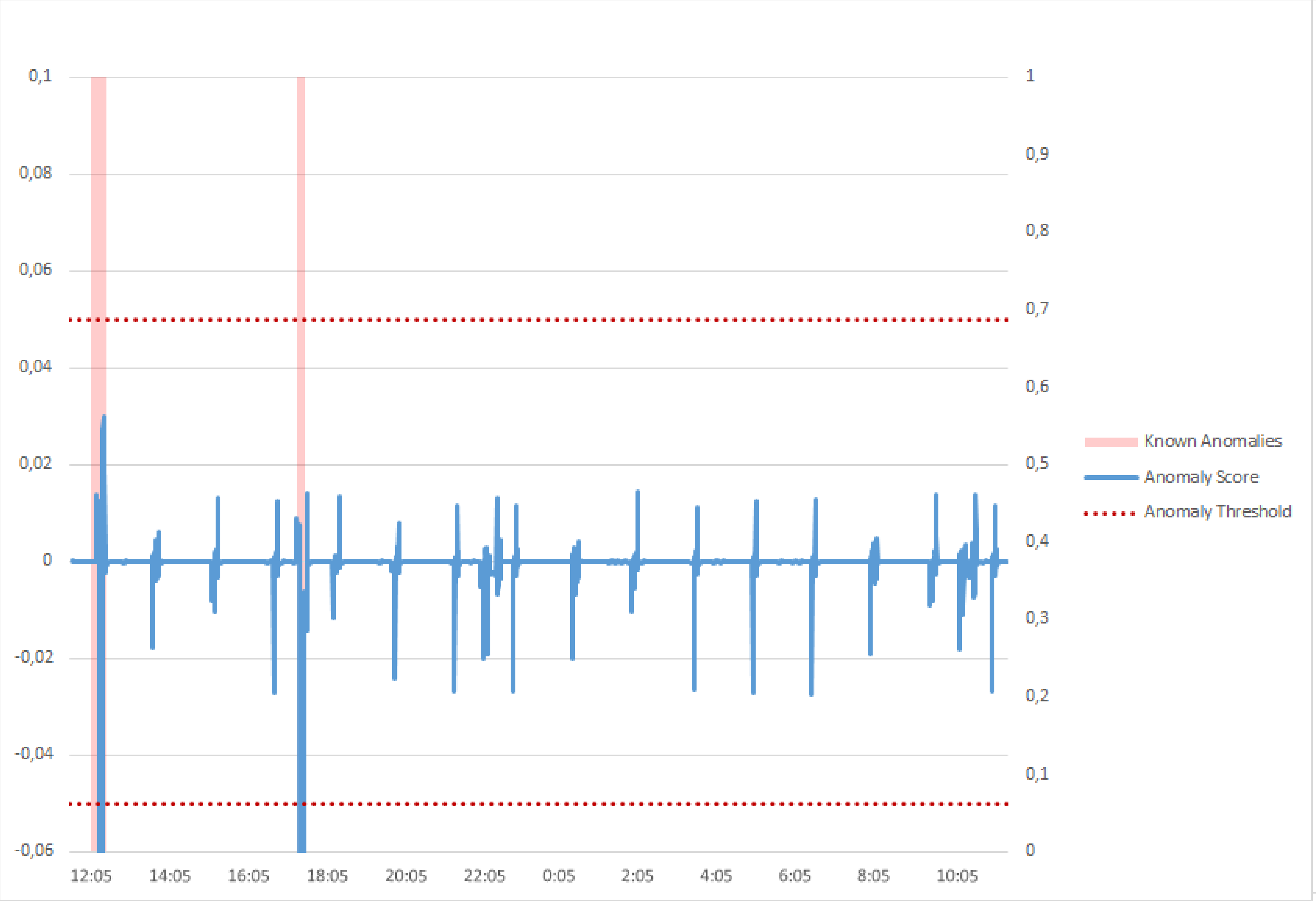
NB. OF PACKETS (5 min): OBSERVED vs. PREDICTED

IHONEY



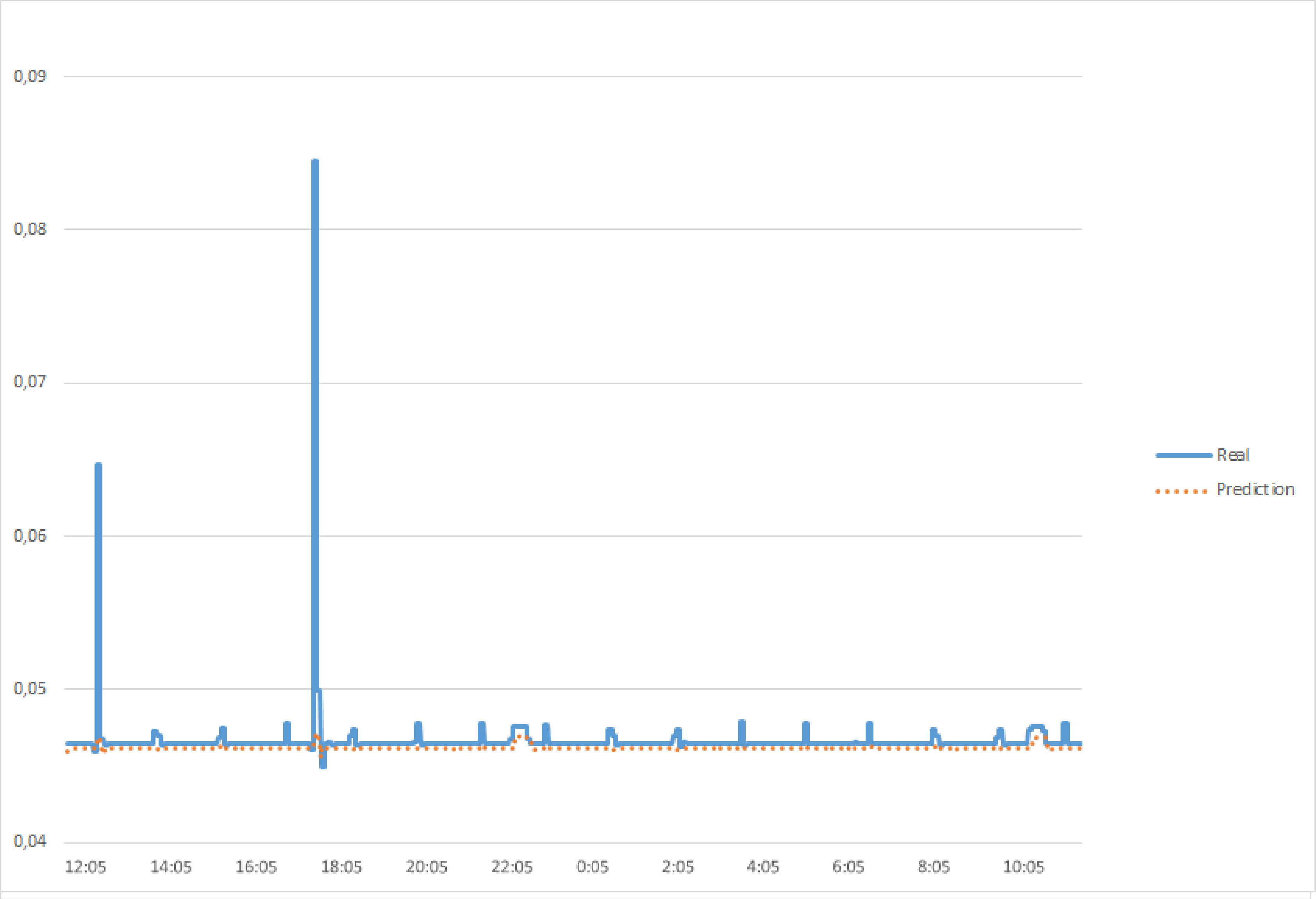
NB. OF PACKETS (5 min): ANOMALY SCORE

IHONEY



AVG. INTER ARRIVAL TIME (5 min): OBSERVED vs. PREDICTED

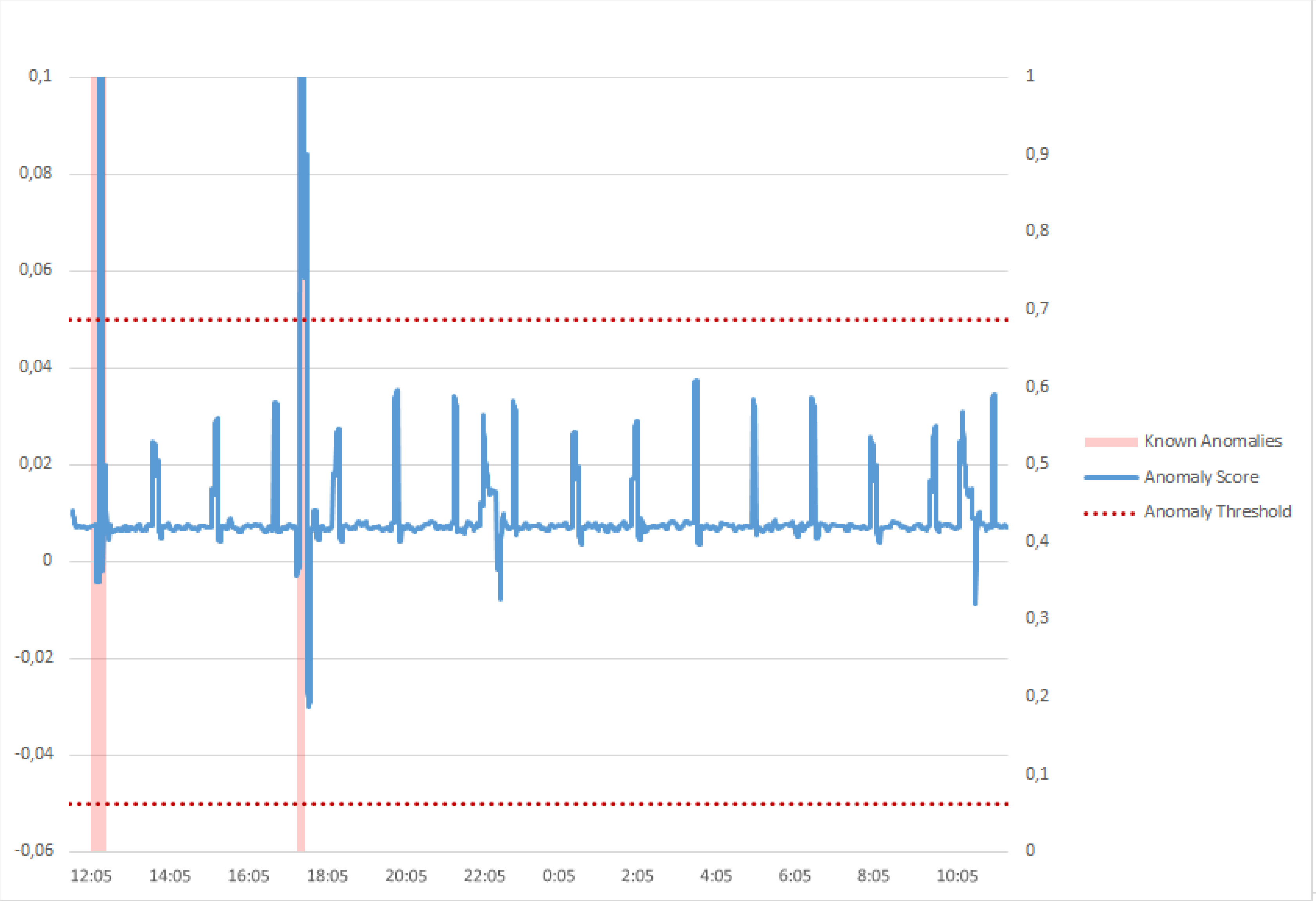
IHONEY



GRUPO

AVG. INTER ARRIVAL TIME (5 min): ANOMALY SCORE

IHONEY



- **Detection capability comparison**
  - Dataset of real attacks registered by the honeypot from 2016
  - 8 traffic captures containing anomalies/attacks
  - Traditional (IDS + PVS) vs Machine Learning
- **Machine Learning models**
  - 10 metrics x 5, 10 and 30 minute time slot aggregation
  - LSTM neural networks + Regression models

Comparison results

- Traditional methods only detected some of the attacks
- ML-based techniques outperform traditional methods
- Method combination/co-relation detected all anomalies

DETECTION	P1	P2	P3	P4	P5	P6	P7	P8
IDS + PVS	✗	✓	✓	✓	✗	✗	✓	✗
ML	✓	✓	✓	✓	✓	✓	✓	✓

CONCLUSIONS AND NEXT STEPS

- **Anomaly detection system**
  - Non-Invasive time slot metrics extraction from network traffic
  - Different Machine Learning models training
  - Classification/Prediction results co-relation
  - ML-Based results outperform traditional approaches
- **Next steps**
  - More metrics: Ml-Based, non-related to network traffic...
  - More ML models: Autoecoders, Restricted Boltzmann Machines

Learning the way analysts work while they do it

- Use *Association Mining* techniques to learn which actions cyber security analysts do when dealing with an alert:

    Alert parameters

    Queries performed

    Previous alerts reviewed

    Similarity between current alert and previous ones

    ...

Association Mining

- Finding frequent patterns, associations, correlations or causal structures among sets of items or objects
- Unsupervised learning: No need for a properly labeled training set
- *Support*: Probability of having A and B together
- *Confidence*: Probability of having B after having A
- *Lift*: Probability of B having a causal relation with A

- **Facts *[1]*:**
  - Worldwide, 37% of organizations face more than 10,000 alerts/month
  - Within the US, 37% of organizations face more than 50,000 alerts/month: more than 1,500 alerts/day, 70 alerts/hour
- **Impossible to review every alert**
- **Important alerts are lost, overlooked or responded too slowly**

[1] 'The Numbers Game: How Many Alerts are too Many to Handle?' – FireEye and the International Data Corporation, 2015

OTHER RESEARCH LINES: LM3

LEVEL 1 ALERT RESOLUTION PROCEDURE

- Check alert data
- Search alert name in alert history
- Found similar alerts in the past
- Filter historical results by source IP
- Found same alert for same source IP address in alert history: It was a false positive
- Change alert EBS to ‘False Positive’
- Copy and paste resolution from past alert
- …

ALERT DATA

- Alert Name
- Src. IP
- Dst. IP
- EBS
- …

LEVEL 1 ALERT RESOLUTION PROCEDURE

- Check alert data
- Search alert name in alert history

Approximately 80% of the queries run and analyses performed manually during alert qualification and validation are IDENTICAL

OTHER RESEARCH LINES: LM3

LEVEL 1 ALERT RESOLUTION PROCEDURE

- Check alert data
- Search alert name in alert history

Approximately 80% of the queries run and analyses performed manually during alert qualification and validation are IDENTICAL

LM3: Low Complexity Man-Machine Module

OTHER RESEARCH LINES: LM3

RECOVERING DATA FOR THE LEARNING ALGORITHM

- Alert data
- Queries made
- Historical alerts consulted
- Historical alerts and current alert similarity
- String analysis

...

ALERT DATA

- Alert Name
- Src. IP
- Dst. IP
- EBS
- ...

OTHER RESEARCH LINES: LM3

ASSOCIATION MINING PROCESS

- Identification of frequent elements
- Calculation of Support, Confidence, Lift values, etc
- Automatic alert resolution of low complexity alerts
- Resolution rule generation for low complexity alerts

RECOVERING DATA FOR THE LEARNING ALGORITHM

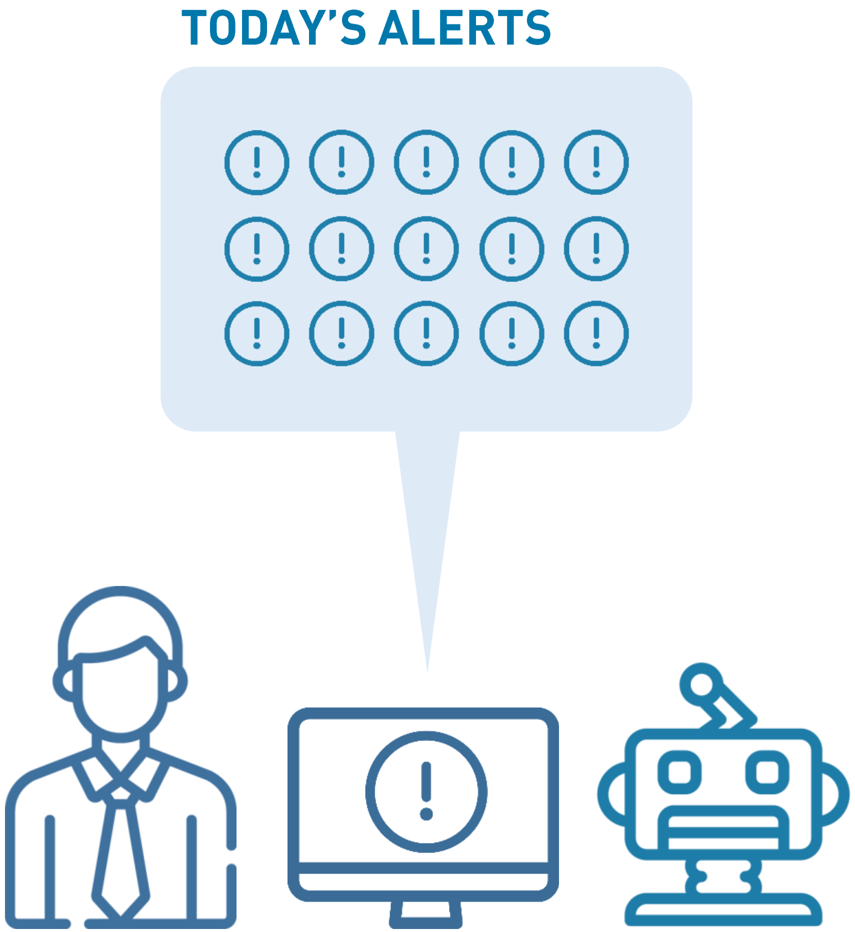
- Alert data
- Queries made
- Historical alerts consulted
- Historical alerts and current alert similarity
- String analysis

...

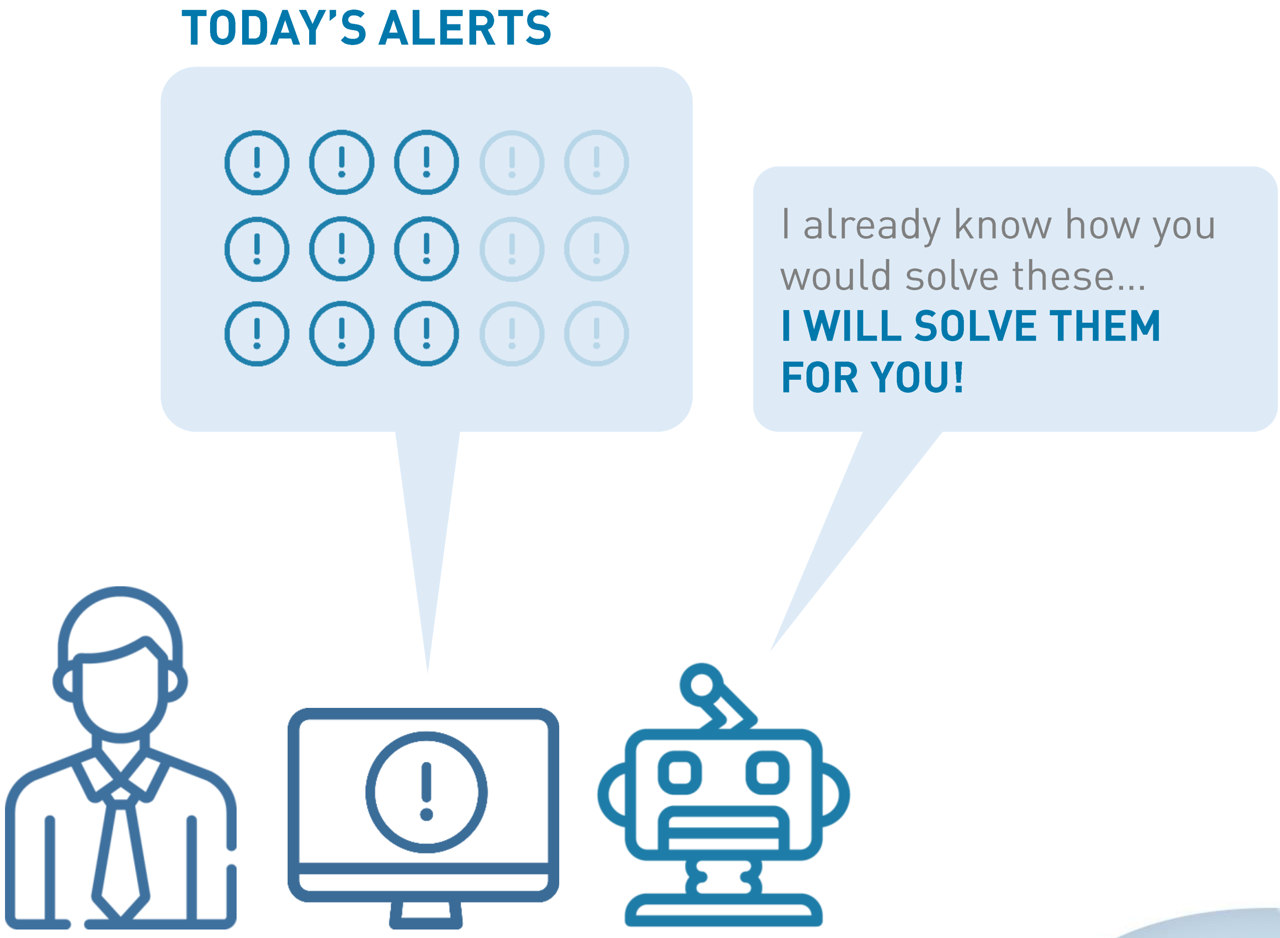
ALERT DATA

- Alert Name
- Src. IP
- Dst. IP
- EBS
- ...

OTHER RESEARCH LINES: LM3

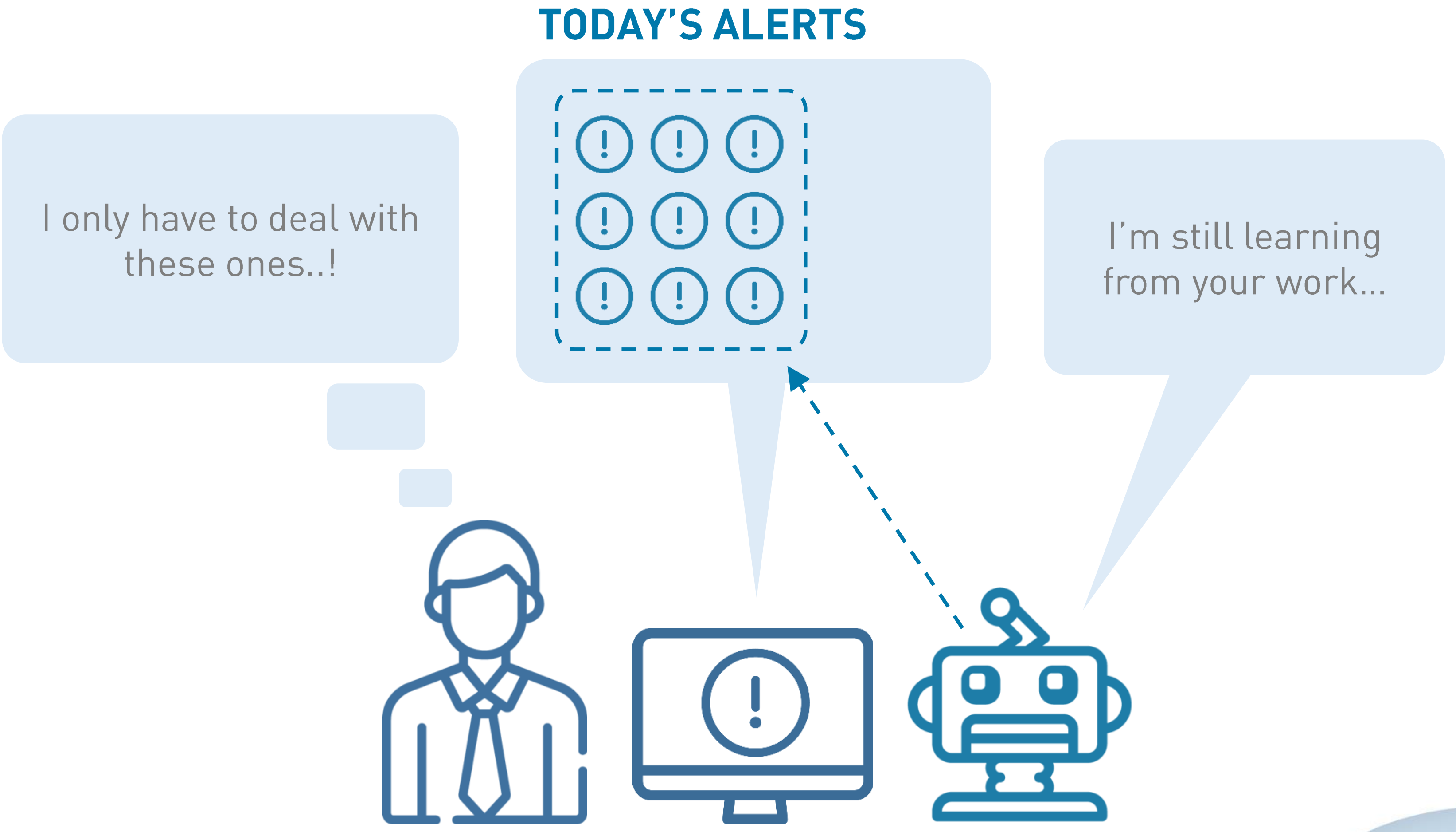


OTHER RESEARCH LINES: LM3



OTHER RESEARCH LINES: LM3

OTHER RESEARCH LINES: LM3



Global impact in SOC

- Low complexity alert resolution procedures are learnt from human analysts
- Low complexity alerts (approximately 40% of level 1 alerts) are then automatically resolved
- Increase of total attended alerts with the same human resources
- Reduction of response times in level 1
- Reduction of probability of human error due to alert fatigue

GRUPO

Anticipating a
cyber secure world

MADRID	BARCELONA	VALENCIA	BRUSSELS	LISBON	BOGOTÁ	MÉXICO D.F.
Velázquez 150, 2ª planta, 28002 T.(+34) 902 882 992	Llull, 321 (Edifici Cinc) 08019 T.(+34) 902 882 992	Ramiro de Maeztu 7, 46022 T.(+34) 902 882 992	Rue belliard 20, 1040 T.(+32) (0) 474532974	Rua Cidade Rabat 27, 1.dto, 1500-159. T.(+35) 1917620918	Carrera 11 Nº93A - 53, Of. 401 T.(+57 1) 74 5 74 39	44-7, México D.F. 06600 T.(+52) 55 2128 068