DFN-CERT

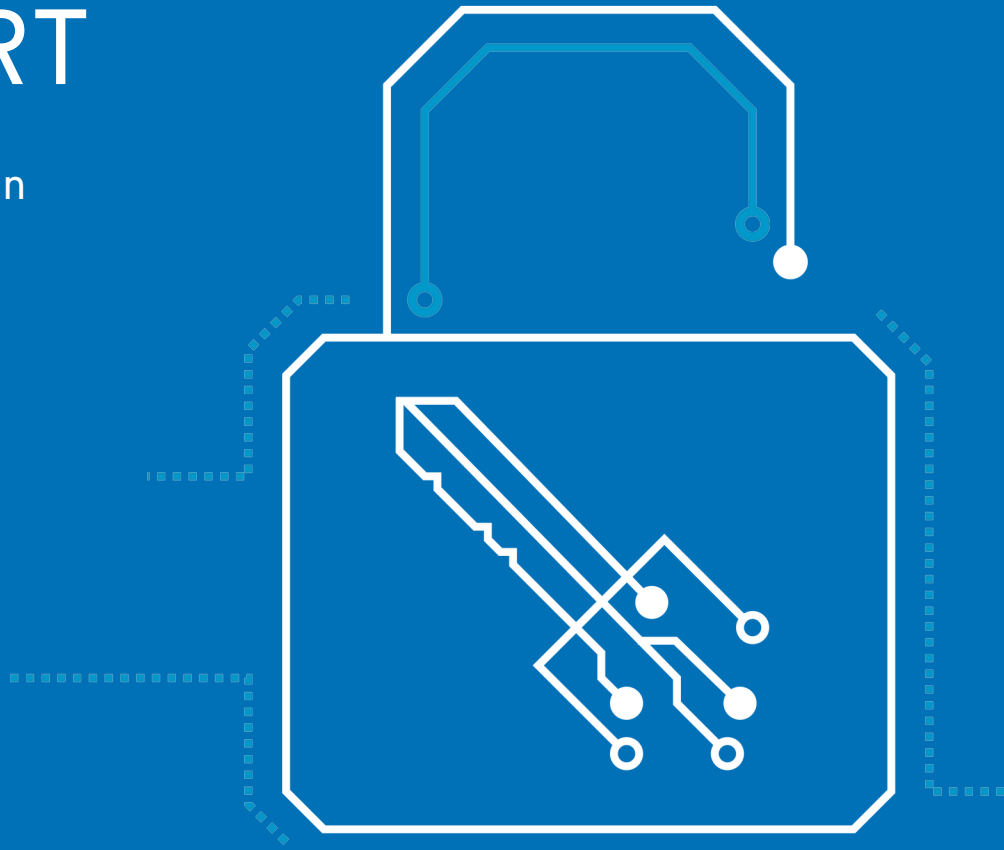
Using Machine Learning approaches to facilitate network situational awareness

1st SIG-AI Meeting December/2024 Poznan

Jan Kohlrausch

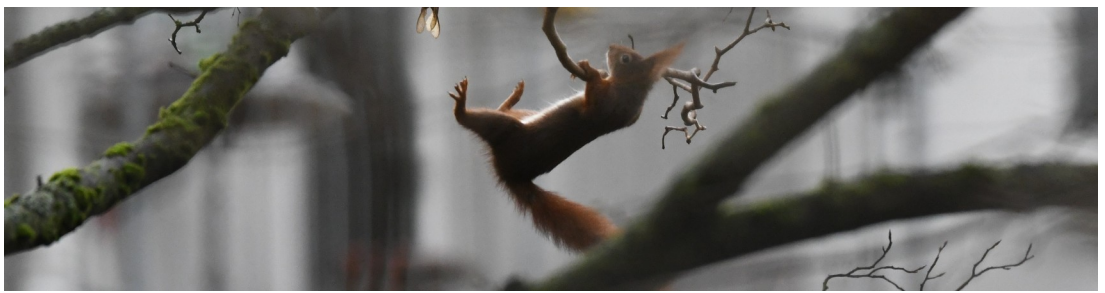
Introduction DFN-CERT

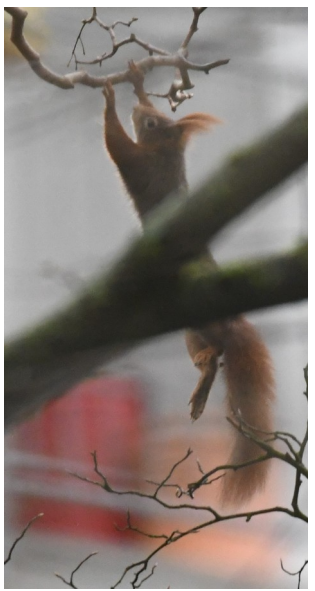
- Computer Emergency Response Team for the German Research Network (DFN)
- Our services for universities and research institutes:
  - Facilitating incident response
  - Security advisory service
  - Sharing Threat Intelligence
  - SOC operation
  - PKI services



Our Challenges and Motivation

- Cope with a very large number of incidents and security compromises:
  - Fast and precise reaction to threats; e.g., DDoS attacks, user account compromises, …
- Large and complex network:
  - Network security awareness is important
  - What is going on in our network? Are there serious threats?
    - Ransomware incidents?
    - Computer worms?
- Automation and fast response is the key to success!
- Improvements by ML and AI (e.g., detection, reaction)?





DFN
DEUTSCHES FORSCHUNGSNETZ

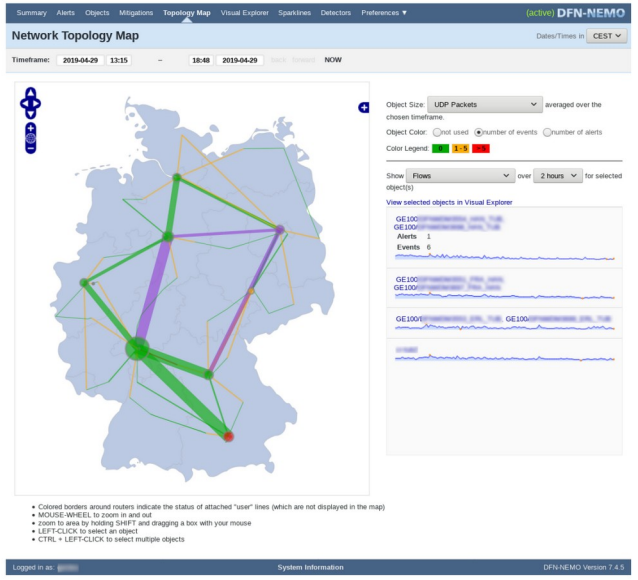
Current Use Cases for ML and AI

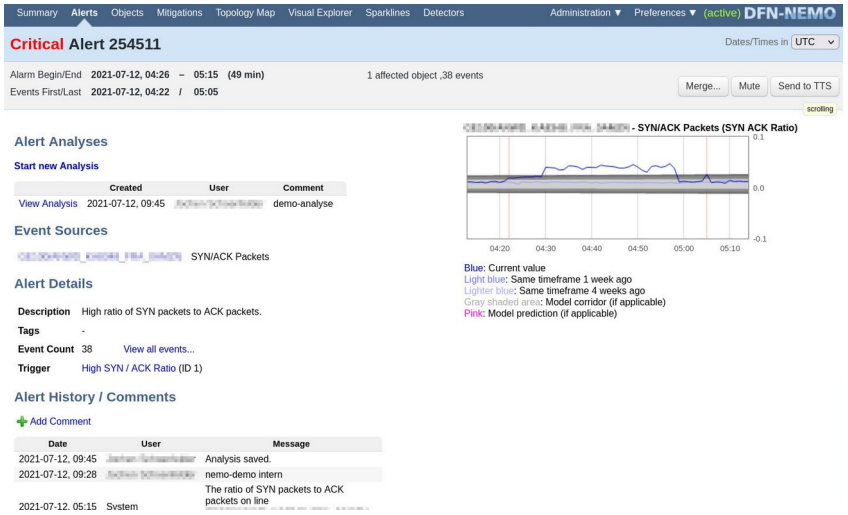
- Apply ML approaches to facilitate network situational awareness
  - Analysis of incident data to detect critical incidents on our network / Internet
  - Understand the impact of critical vulnerabilities: exploitation behavior
- Supporting detection and mitigation of DDoS attacks
  - Anomaly detection in network traffic

DFN
DEUTSCHES FORSCHUNGSNETZ

Network Monitoring (NeMo)

- Modeling the network to get an overview of connections and benign traffic volumes
- Supporting detection of DDoS attacks using Holt-Winters exponential smoothing for traffic prediction and anomaly detection
- Using threshold as an alternative solution and customization option

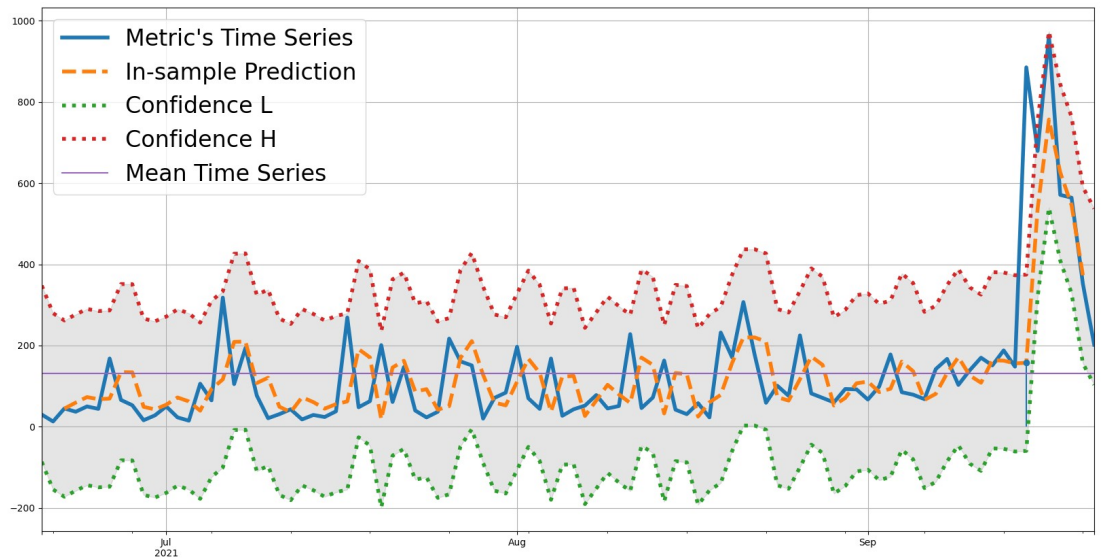




DFN
DEUTSCHES FORSCHUNGSNETZ

Network Situational Awareness

- Application of time series analysis to detect anomalies in attack activity: ARIMA models: Scans for the OMIGOD vulnerability in the MS Azure Open Management Infrastructure (OMI).



Number of targets being attacked on port TCP/1270 (ISC data) and ARIMA analysis (in-sample prediction and confidence interval)

DFN
DEUTSCHES FORSCHUNGSNETZ

Summary and lessons learned

- Automation of incident response/coordination and network traffic analysis is our key to success
- Can be supported by approaches from AI / ML:
  - Detection of attacks and/or incidents
  - Providing network situational awareness
- Deployment of approaches for time series analysis:
  - ARIMA can model attack/incident numbers to detect anomalies
  - Holt-Winters allows to detect anomalies in network traffic volume

→ Currently, not mission critical, but it works!

DFN
DEUTSCHES FORSCHUNGSNETZ

The Future

- Extend our existing approaches and initiatives
  - Application in our SOC service (e.g., anomaly detection on log messages)
  - Use more complex models, e.g., SARIMAX or approaches from deep learning (LSTM)
- Explore new opportunities:
  - Use gen-AI (LLMs) to produce playbooks for incident response
  - Use gen-AI to support our security advisory service
  - Apply LLMs to classify and manage threat reports
  - Prepare for new attacks involving gen AI:
    - AI-based classification methods to detect deep fakes and AI generated content (e.g., Phishing)

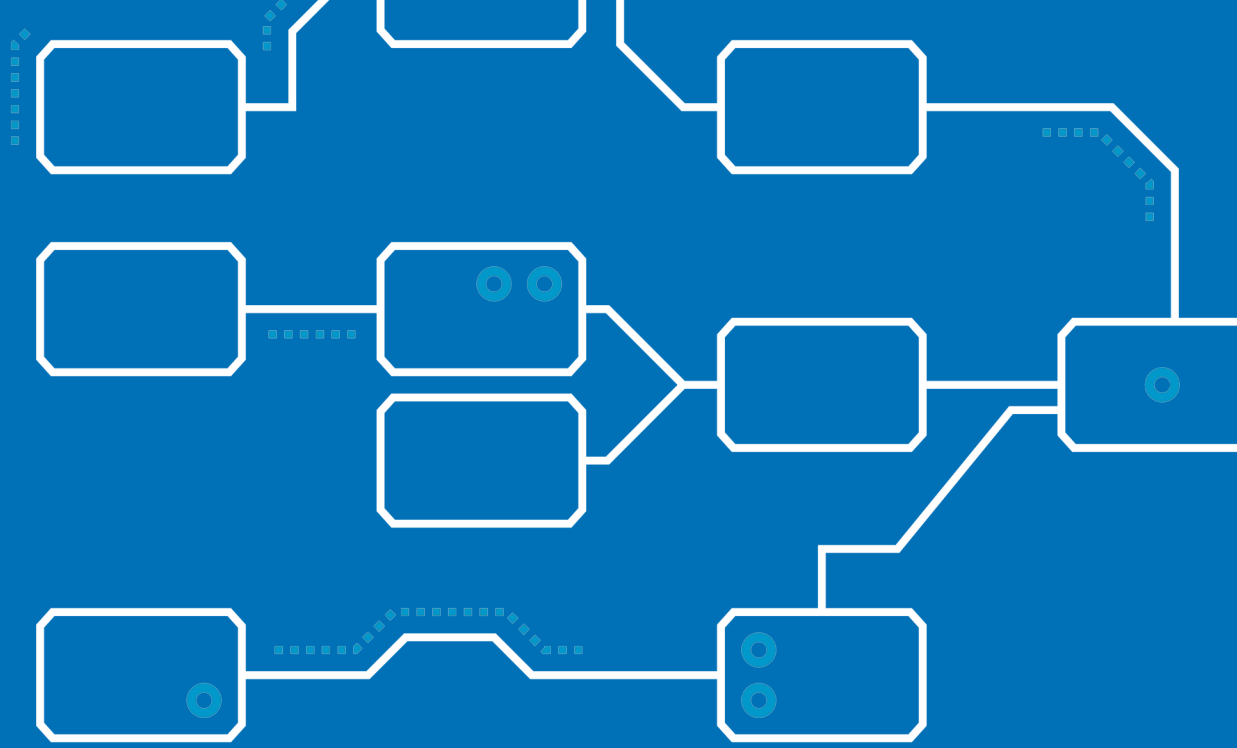
DFN
DEUTSCHES FORSCHUNGSNETZ

The all-important question

Will Artificial Intelligence – specifically generative AI – become a game changer?

→ let's find out!

DFN
DEUTSCHES FORSCHUNGSNETZ



Many Thanks! Questions?

DFN-CERT