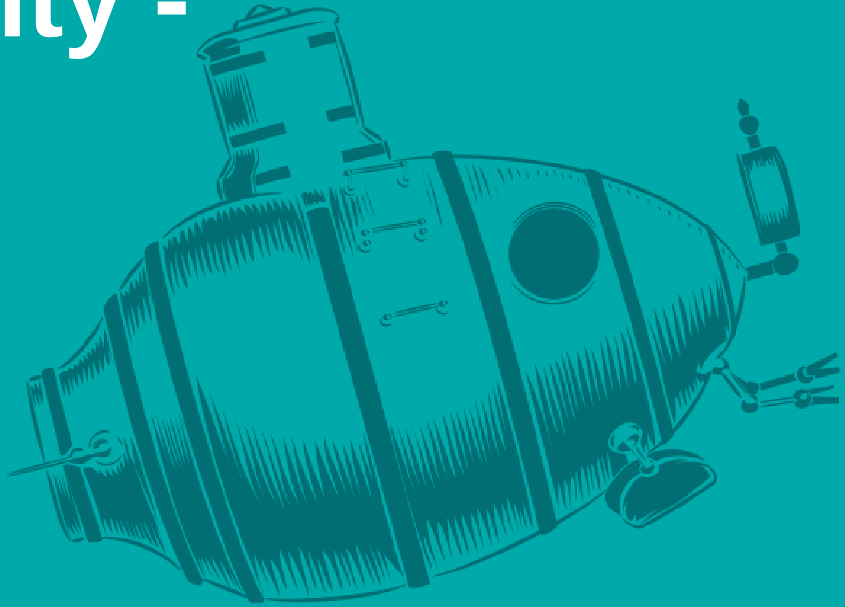
ALEF

AI in cybersecurity - now and then



Lukáš Mečíř

Splunk SIEM / Security Expert, ALEF NULA

lukas.mecir@alef.com

Introduction

Lukáš Mečíř
Splunk SIEM/Security Expert

splunk> CERTIFIED Splunk Enterprise Security Certified Admin

splunk> CERTIFIED Splunk Enterprise Certified Admin

splunk> CERTIFIED Splunk Enterprise Certified Architect

splunk> Partnerverse SELL ELITE

Who is who

Artificial Intelligence

- technology that enables computers and machines to simulate human intelligence and problem-solving capabilities like learning, planning, **creativity**,…

Machine Learning

- technology that uses algorithms and statistical models to process data and improve the performance of certain tasks

Deep Learning

- a type of machine learning that uses neural networks to learn from large amounts of data and the results of its own activities

Generative AI

- creates content based on statistical data processing (Large Language Models - LLM)

Role of AI / ML in Cybersecurity

Predictive / Reactive	Generative
(Machine Learning / Deep Learning)	*(Generative AI - ChatGPT like)*
Detect attack	**Interact with people to speed up / ease work**
Stop attack automatically	**Does not stop attack**
Machine speed, no human slowness	
	Helping make sense of occured alerts
Automation of defense early in killchain	Helping with further investigation
Zero-day attacks - Lateral movements	*Investigation assistance - TI context*

Using ML / DL in cybersecurity

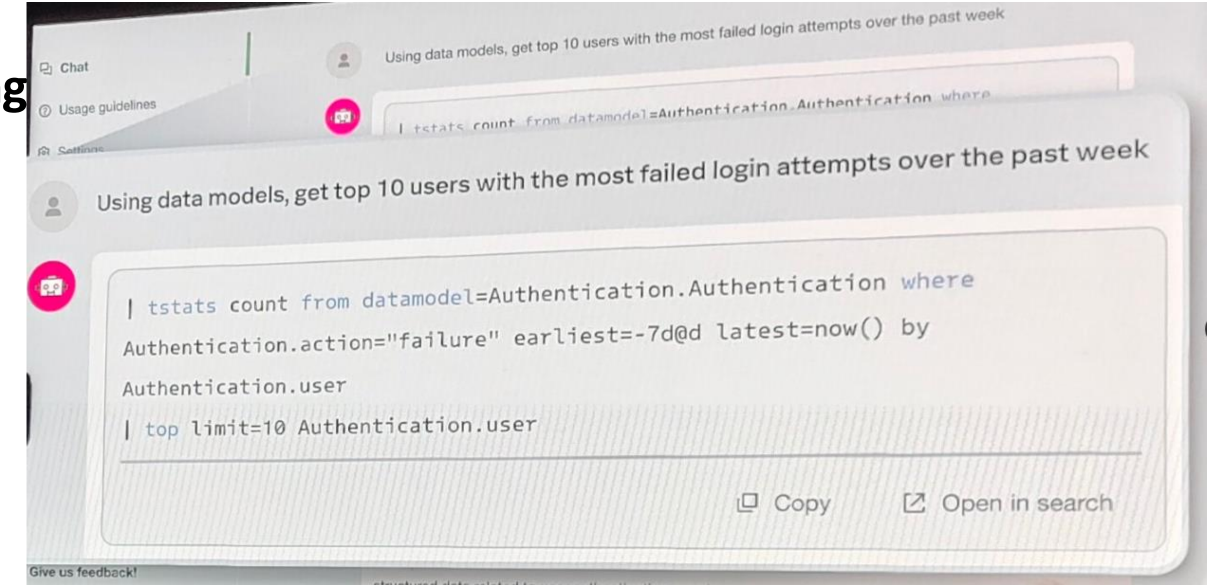
Use Case	Anomaly Detection	Predictive Analysis	Clustering	Graph Analysis
User Access Anomalies	✓			
Potential Insider Threats	✓		✓	
Domain Generation Algorithms (DGA)s		✓		
Command Line Anomalies	✓	✓		
ML based Threat Hunting	✓		✓	✓
Malicious Network Traffic Patterns	✓			
Fraudulent Activity	✓		✓	✓

Alerts Corellation

- **Second level of analyzing -analyzing alerts**
- **Grouping alerts**
- **Patterns matching**
- **Risk Based Alerting**

Generation AI in Cybersecurity

- Information collecting
- Symplifying further investigation - creating searches etc.



Using data models, get top 10 users with the most failed login attempts over the past week

```
| tstats count from datamodel=Authentication.Authentication where
Authentication.action="failure" earliest=-7d@d latest=now() by
Authentication.user
| top limit=10 Authentication.user
```

AI Considerations

- Purpose built AI for optimal outcomes
- Humans belong in the driver’s seat, with AI as a trusted copilot
- Openness and extensibility (vs. model poisoning / stealing)
- AI content
  - Out-of-the box ML (SIEM)
  - Pre-defined threat detection modeling (UEBA)
  - “Mission guidance” (SOAR)
  - ML powered tools for malicious code analyzing (Attack Analyzer,…)
- Usability, user experience

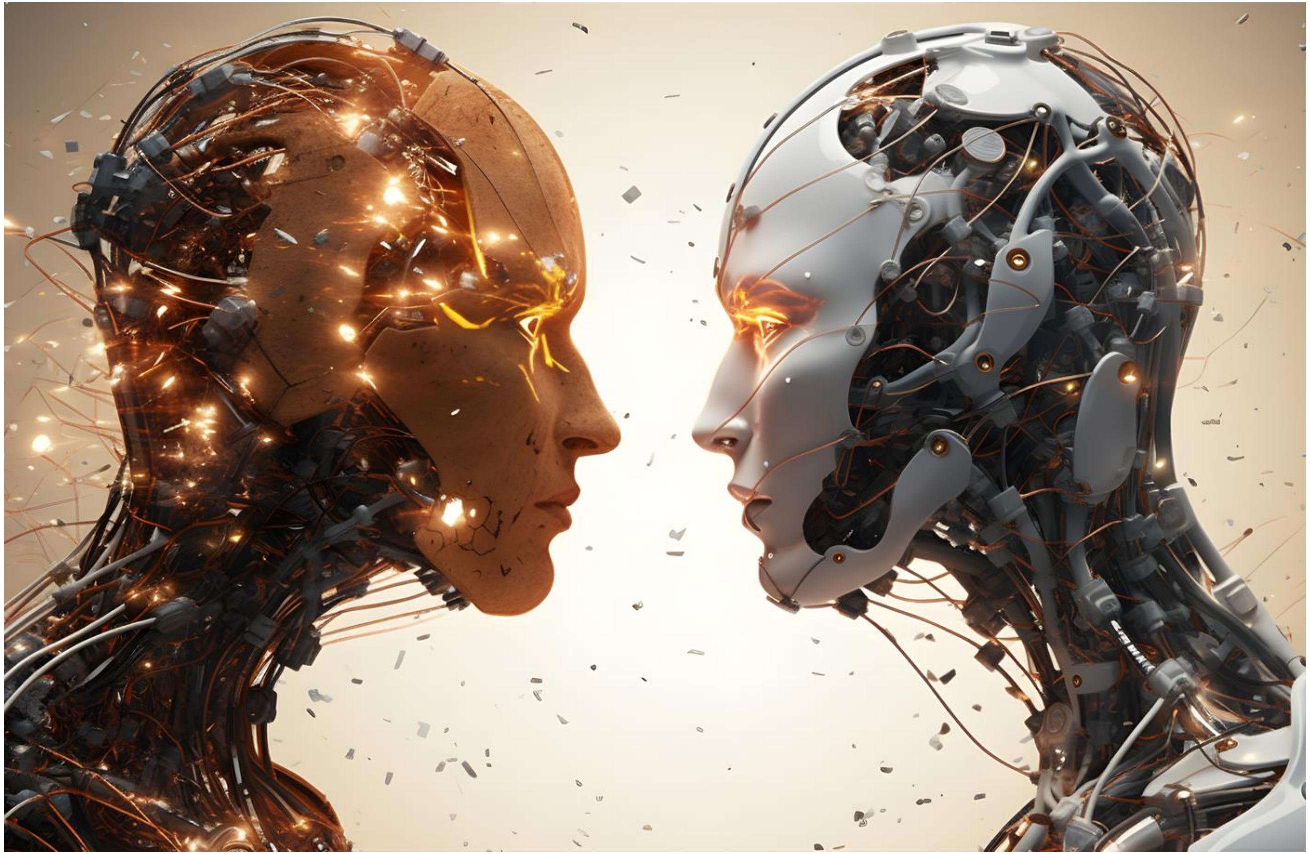
AI future - Bad guys

- Ramnit - malware modules dowloaded based on particular device
- Emotet - Running processes analysis before malicious code starts
- FraudGPT, WormGPT, Wolf GPT, DarkGemini…
- Keylogger made by ChatGPT prompt (ESET Research)
- Deep Learning usage - dynamic and responsive attack

AI future - Good guys

- Security specific insights
- Context into Security monitoring environment
- Tight integration into Security workflow
- Integration between monitoring and response
- Monitoring of using AI tools
- Deep Learning usage - Dynamic response - Autonomous Cybersecurity Systems

AI vs AI?



ALEF

Děkuji za pozornost

Lukáš Mečíř
Splunk SIEM / Security Expert, ALEF NULA
lukas.mecir@alef.com