THE FUTURE OF HYBRID AI

Combining Local and Cloud-Based Models for Cybersecurity

Speaker Intro

- Sven Vetsch
- Redguard AG
  - Co-founder
  - Head of Innovation & Development
- Working in information security for ~17 years
- AI/ML cybersecurity research since ~6 years

Contact: sven.vetsch@redguard.ch

The Cybersecurity Landscape

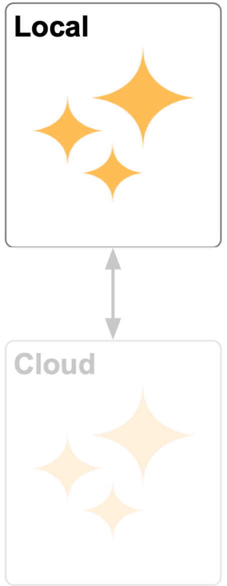
- Increasingly sophisticated, targeted threats
    - Attackers leverage advanced evasion techniques and zero-day exploits tailor-made to specific victims.
- Massive data growth from IoT and edge devices
    - Billions of connected devices generate vast amounts of security-relevant data.
- Need for real-time, proactive security
    - Detection and response need to be lightning-fast to outpace cyberattacks and minimize damage.

AI's Potential and Challenges

- Advanced threat detection and pattern recognition
  - AI excels at finding anomalies and hidden attack patterns in enormous datasets.
- But... centralization raises concerns:
  - **Privacy risks:** Centralized models require pooling sensitive data.
  - **Latency in cloud communication:** Delays can hinder real-time response.
  - **Potential single point of failure:** Over-reliance on cloud connectivity can create new problems and vulnerabilities.

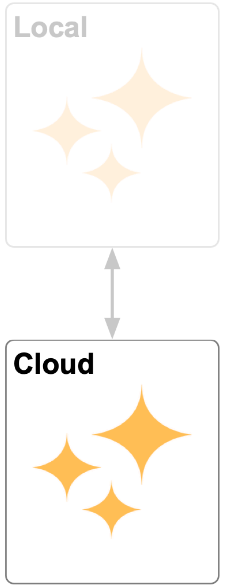
The Power of Local AI Models

- **Privacy:** Data never leaves the device (or local environment)
- **Speed:** Immediate anomaly detection
- **Customization:** Adapt to the unique user/device behavior and environment
- **Resilience:** Less reliance on cloud connectivity



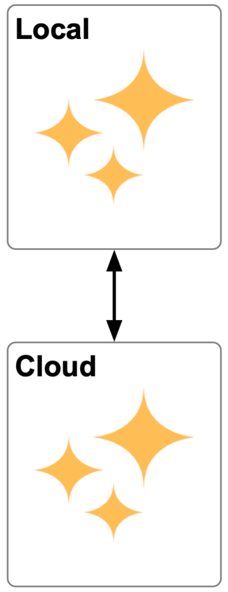
Advantages of Cloud-Based AI

- **Scalability:** Handle massive datasets and complex models
- **Collaboration:** Learn from patterns across a wide range of devices and users
- **Updates:** Rapid deployment of new defenses against evolving threats



The Hybrid AI Approach

- Synergistic combination of local and cloud AI
- **Intelligent Partitioning:** Decide what tasks run where
  - Local: basic anomaly detection, privacy-sensitive tasks
  - Cloud: complex analysis, threat signature updates
- **Privacy-Preserving Sharing:** Federated learning, differential privacy



Technical Considerations

- **Model Partitioning:** Deciding which AI layers execute locally vs. in the cloud
  - Factors: Device capabilities, privacy requirements, computational cost
- **Secure Communication:** Protocols for efficient and protected data exchange
  - Explore encryption, compression methods tailored to this context
- **Privacy-Enhancing Techniques:**
  - Federated learning: Train models across devices without revealing raw data
  - Differential privacy: Introduce noise for statistical analysis

Hybrid AI Use Cases

- **Network intrusion Detection:** Local monitoring + cloud-based threat correlation
- **Personalized Malware Protection:** Local adaptation alongside cloud updates
- **Collaborative Threat Intelligence:** Devices flag anomalies for cloud analysis
- **IoT Security:** Local real-time anomaly detection, cloud for global threat intelligence
- **Privacy-Preserving Surveillance:** Local image recognition, cloud-based pattern matching
- **Healthcare Security:** Local patient monitoring, cloud-based disease pattern recognition

... and many more!

Challenges & Research Directions

- **Explainability of Hybrid Decisions:** Understanding how local & cloud AI interact
- **Resilience Beyond Attacks:** Fault tolerance, recovery in hybrid models
- **Adversaries in a Hybrid World:** Attacks targeting the distributed architecture
- **Real-World Benchmarking:** Need for standard datasets and evaluation methods

Conclusion

- Hybrid AI: A key strategy for intelligent, privacy-aware, proactive cybersecurity.
- Call to action: Explore hybrid models for your security challenges.

REDGUARD
SECURING YOUR ASSETS

Thank you for your attention