



Make your AI Systems

**R**obust, **R**esponsible and **R**eliable

Get a 360 degrees view of vulnerabilities of your AI systems  
Demonstrate trustworthiness of your machine learning engines  
Comply with AI privacy and regulatory requirements

**Cyber****Orion**

# Finding **Vulnerabilities** in Your AI Engines

**Regular AI  
Vulnerability  
Scanning**



AI services are becoming the corner stones for many businesses in the 21st century. AI systems may make wrong things, learn wrong things, or reveal wrong things!

Making sure that your AI systems are safe and secure and you are in control of your AI services would minimize the risk to your business and protect your brand and reputation.

**Image & Video  
Recognition  
Vulnerability  
Testing**

**Text-Analysis  
AI Systems  
Vulnerability  
Assessment**

**Audio-based  
AI Systems  
Testing**

**Cloud  
AI Systems  
Testing**





# Secure Your **AI** Data Pipeline

**Trust** is the cornerstone of your company's reputation. Reliability, fairness, interpretability, and robustness of the AI data pipeline are essential to guarantee the trustworthiness of your AI systems.

Business decision-makers need to prioritize AI and automation related activities and identify the level of investment required to build a robust ethical and trustworthy AI ecosystem.



- **Receive an expert estimate of your AI systems security maturity level**
- **Limit your exposure to unknown adversarial attacks**
- **Benchmark your AI services against your peers**

# Guarantee Compliance of AI Services and **Privacy** of Your Information



- ✓ AI Privacy Risk Assessment
- ✓ AI Compliance with PCI-DSS
- ✓ AI Compliance with ISO27001
- ✓ AI Alignment with Canada's Responsible Use of Artificial Intelligence guideline
- ✓ AI Alignment with the EU Ethics Guideline for Trustworthy AI

Complex deep learning systems inherently lack transparency and explainability and may infringe upon legal or regulatory verification. AI services are increasingly playing a critical role in many businesses that require compliance with different security standards, **a significant challenge for many businesses.**



# Realize the Full Potential of **Ethical AI** in Your Industry

## Transport

AI has significantly impacted the transportation sector and widely applied in different domains. Transportation systems operate in a domain that is anything but simple. Even most robust AI-systems require continuous security monitoring when deployed in such a sophisticated environment.

We help data collectors, solution developers, service deployers and consumers in this domain to build, deploy and use safe, secure, and reliable AI systems.

## Healthcare

AI has already improved diagnosis accuracy, reduced required time to determine cause and course of disease, and helped in formulating an effective treatment for diseases.

To be trustable, healthcare-AI systems should offer a high degree of transparency and explainability without risking privacy of data that is used to train those systems.

We offer a range of services to assure safety and privacy of AI engines that are used in the healthcare sector and assure their compliance with security standards and regulatory requirements.

## Finance

AI has been widely used in the financial sector for client risk profiling, fraud detection, credit risk evaluation, and for automating manual processes. It is important to make sure that these AI engines are secure, robust, unbiased and fairly treating all customers.

Our AI-Security scientists work closely with cybersecurity team in banking and financial sector to assess robustness of AI systems and to assure their compliance with security and regulatory requirements.

# Why **CyberOrion**?

**Based in the Royal City of Guelph, Ontario, Canada, **CyberOrion** works closely with organizations all around the globe to make their machine learning services **Robust, Responsible and Reliable.****

Call : +1 - (647) -

Email : [info@CyberOrion.com](mailto:info@CyberOrion.com)

URL: [www.CyberOrion.com](http://www.CyberOrion.com)