# How to Mitigate AI Risk

Artificial Intelligence is becoming more and more ubiquitous in today's world. There are positives to learning how to use AI, but there are also risks to watch for.
Here are some ways to Mitigate AI Risk!

## Deploy AI-Enhanced Threat Detection and Response

Use AI to monitor network behavior, detect anomalies, and respond to threats in real time. This can include predictive analytics and automated containment to reduce response time and damage.

## Enchance Data Governance and Soverignty

Establish strict controls over data access, quality, and compliance. This can include automated data management tools and frameworks that ensure privacy and regulatory alignment.

## Adopt a Zero Trust Architecture (ZTA)

Make steps toward implementing a "never trust, always verify" model. This way every user and device must be authenticated and continuously validated, regardless of location or role.

## Integrate AI Into Incident Response Plans

Update your cybersecurity Incident Response Processes to include AI-driven simulations and decision-making tools. This will help in quicker threat triage and enchanced accuracy during root cause analysis.

## Conduct Regular Shadow AI and Vendor Audits

Monitor for unauthorized AI tools (shadow AI) and ensure vendors are transparent about their AI usage. Regular configuration reviews and vendor assessments are essential to success of this process.

## Invest in AI Awareness and Cross-Functional Training

Foster collaboration across departments and train staff to understand both the risk and benefits of AI. This inclues awareness of phishing tactics, data misuse, ethical AI deployment, etc.