

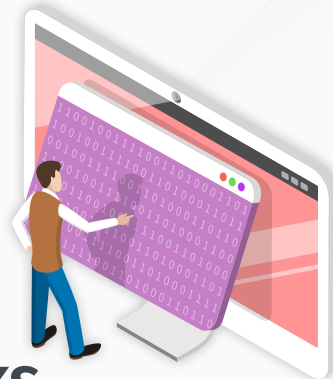
# GENERATIVE AI IN CYBERSECURITY

AI technologies are essential in detecting and responding to emerging cyber threats. This factsheet provides strategies for effectively leveraging AI in cybersecurity.



## BENEFITS

- Rapidly identifies and responds to new threats.
- Automates incident response, reducing reaction time.



## RISKS

- Over-dependence on AI for critical decisions.
- Security and ethical concerns.

### Tips for Using AI in Detecting and Responding to Cyber Threats



#### Enhanced Detection Capabilities

AI-driven analytical tools are capable of detecting subtle anomalies in system behavior that may indicate security breaches.



#### Automated Incident Response

Develop AI-informed incident response plans that include scenarios involving AI systems as both the target and tool of cyber-attacks.



#### Proactive Threat Intelligence

AI-based threat intelligence can anticipate and prepare for potential cyber threats. AI can analyze patterns and predict future attacks more rapidly, allowing for proactive defense strategies.



#### Maintain Human Collaboration

Ensure that AI systems work alongside human security teams. AI can provide valuable insights, but human expertise is crucial for interpreting and acting on these insights.



#### Regular Training

Keep AI tools and security teams updated with the latest threat intelligence and AI advancements. Regular training and updates are essential for maintaining an effective cybersecurity posture.