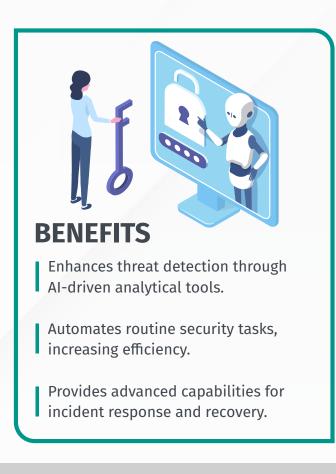
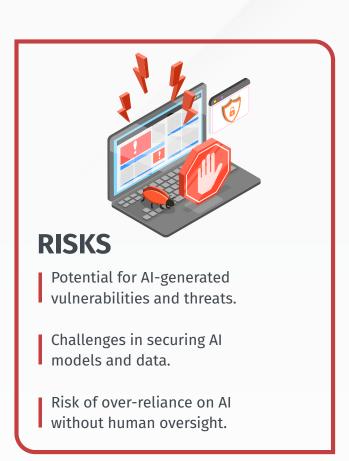
GENERATIVE AI IN CYBERSECURITY

Generative AI (GenAI) has the opportunity to revolutionize cybersecurity though automated threat detection and response capabilities. However, its adoption also introduces unique risks that need to be managed proactively. This factsheet outlines key considerations and strategies for leveraging GenAI in cybersecurity.





Tips for Leveraging Generative AI in Cybersecurity



Adopt a Proactive Security Methodology

Implement a comprehensive approach encompassing governance, identification, protection, detection, response, and recovery. This multilayered defense strategy addresses GenAl's unique vulnerabilities.



Understand and Address GenAI-Specific Risks

Develop awareness and training programs to mitigate adoption risks, conduct regular vulnerability assessments, and prepare for potential misuse of GenAI by adversaries.



Prioritize Data Security and Integrity

Enhance data management practices, implement advanced monitoring and access control, and use encryption and anonymization techniques to protect AI training data.



Brace for Emerging GenAl Threats

Establish robust validation processes, provide continuous security training, and engage in collaborative threat intelligence to stay ahead of new AI-related vulnerabilities.



Leverage GenAl to Strengthen Defenses

Integrate GenAI into security processes for automation, advanced threat detection, and dynamic risk management. Promote a culture of continuous learning and collaborative analysis.

