Sikos

# Generative AI in Cybersecurity


This book explores the most common generative AI (GenAI) tools and techniques used by malicious actors for hacking and cyber-deception, along with the security risks of large language models (LLMs). It also covers how LLM deployment and use can be secured, and how generative AI can be utilized in SOC automation.

The rapid advancements and growing variety of publicly available generative AI tools enables cybersecurity use cases for threat modeling, security awareness support, web application scanning, actionable insights, and alert fatigue prevention. However, they also came with a steep rise in the number of offensive/rogue/malicious generative AI applications. With large language models, social engineering tactics can reach new heights in the efficiency of phishing campaigns and cyber-deception via synthetic media generation (misleading deepfake images and videos, faceswapping, morphs, and voice clones). The result is a new era of cybersecurity that necessitates innovative approaches to detect and mitigate sophisticated cyberattacks, and to prevent hyper-realistic cyber-deception.

This work provides a starting point for researchers and students diving into malicious chatbot use, system administrators trying to harden the security of GenAI deployments, and organizations prone to sensitive data leak through shadow AI. It also benefits SOC analysts considering generative AI for partially automating incident detection and response, and GenAI vendors working on security guardrails against malicious prompting.

This book explores the most common generative AI (GenAI) tools and techniques used by malicious actors for hacking and cyber-deception, along with the security risks of large language models (LLMs). It also covers how LLM deployment and use can be secured, and how generative AI can be utilized in SOC automation.The rapid advancements and growing variety of publicly available generative AI tools enables cybersecurity use cases for threat modeling, security awareness support, web application scanning, actionable insights, and alert fatigue prevention. However, they also came with a steep rise in the number of offensive/rogue/malicious generative AI applications. With large language models, social engineering tactics can reach new heights in the efficiency of phishing campaigns and cyber-deception via synthetic media generation (misleading deepfake images and videos, faceswapping, morphs, and voice clones). The result is a new era of cybersecurity that necessitates innovative approaches to detect and mitigate sophisticated cyberattacks, and to prevent hyper-realistic cyber-deception.This work provides a starting point for researchers and students diving into malicious chatbot use, system administrators trying to harden the security of GenAI deployments, and organizations prone to sensitive data leak through shadow AI. It also benefits SOC analysts considering generative AI for partially automating incident detection and response, and GenAI vendors working on security guardrails against malicious prompting.

**48,14 €**
44,99 € (zzgl. MwSt.)

*Lieferfrist: bis zu 10 Tage*

**Artikelnummer:** 9783032052490
**Medium:** Buch
**ISBN:** 978-3-032-05249-0
**Verlag:** Springer
**Erscheinungstermin:** 16.11.2025
**Sprache(n):** Englisch
**Auflage:** Erscheinungsjahr 2025
**Serie:** SpringerBriefs in Cybersecurity
**Produktform:** Kartoniert
**Gewicht:** 143 g
**Seiten:** 71
**Format (B x H):** 155 x 235 mm



**Kundenservice Verlag Dr. Otto Schmidt KG**
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)