Cheatsheet: Generative AI for Cybersecurity

You can explore the provided sample prompt instructions using either sample data or your own real-time data for experimentation.

Task	Sample Prompts
Malware Behavior Analysis	1. Examine the behavior of a given malware sample. 2. Generate a detailed report on the malware's functionalities. 3. Explore any evasion or obfuscation techniques employed.
Email-Based Phishing Assessment	1. Investigate a suspected phishing email. 2. Perform a comprehensive analysis of links, attachments, and content. 3. Identify social engineering techniques employed in the email.
Malicious Document Scrutiny	1. Analyze a document (Word or PDF) suspected of carrying malware. 2. Investigate macros, embedded scripts, and hidden elements. 3. Provide a breakdown of the document's structure and potential risks.
Post-Incident Malware System Review	1. Conduct a post-incident analysis of a system infected with malware. 2. Identify the initial entry point and propagation methods. 3. Evaluate the overall impact on the compromised system. 4. Explore persistence mechanisms used by the malware and indicators of compromise.
Sentiment-Powered Content Moderation	1. Develop a content filtering algorithm for a social media platform that identifies and blocks offensive language and imagery. 2. Implement real-time monitoring to dynamically adjust filtering thresholds based on user interactions and evolving community standards. 3. Create a content moderation system that leverages sentiment analysis to identify offensive content in user-generated posts and comments. 4. Train the system to recognize nuanced expressions, sarcasm, and cultural context to avoid false positives and negatives.
Context-Aware Content Moderation	1. Create a content moderation system that considers the contextual relevance of content, preventing censorship of educational or informative materials. 2. Utilize natural language processing and contextual analysis to understand the intent behind words and phrases within specific contexts. 3. Enable users to provide feedback on moderation decisions, fostering a continuous improvement loop for the filtering algorithms.
Digital Forensics and Incident Response	1. Simulate a cyber incident scenario and perform digital forensic analysis to identify the root cause, tactics, techniques, and procedures (TTPs) employed by the attacker. 2. Generate a comprehensive forensic report detailing the evidence collected, timeline of events, and recommendations for mitigation.
Threat Hunting	1. Initiate proactive threat hunting exercises in a simulated environment to identify potential threats or anomalies within the network. 2. Summarize the findings in a detailed report, highlighting patterns, anomalies, and potential indicators of compromise (IoCs).
Ransomware Incident	1. Simulate a ransomware incident and conduct forensic analysis to understand the ransomware's entry point, lateral movement, and encryption activities. 2. Generate a concise summary report outlining key findings, impact assessment, and lessons learned for future prevention and response.
Cyber Threat Playbook	1. Design a set of incident response playbooks for a variety of cyber threats, including malware infections, phishing attacks, and DDoS incidents. 2. Ensure the playbooks are comprehensive, covering detection, containment, eradication, recovery, and lessons learned for each threat type.
Incident Report	1. Craft a narrative-style incident response report, turning technical details into a compelling story that is accessible to non-technical stakeholders. 2. Focus on key insights, impact on the organization, and lessons learned, making the report informative and engaging for a diverse audience. 3. Create playbooks that align with the incident narrative, emphasizing communication strategies and coordination among response teams.
Incident Triage	1. Triage potential security incidents based on incoming alerts and reports, prioritizing them according to their severity and potential impact. 2. Develop a streamlined triage process that incorporates automation and orchestration to handle a high volume of incidents effectively.

Task	Sample Prompts
Investigative Support Analyst	1. Assist ongoing investigations by collecting, analyzing, and correlating relevant data from multiple sources, including logs, endpoints, and network traffic. 2. Collaborate with incident response teams to provide additional context and insights, helping to uncover the full scope of security incidents.
Vulnerability Management Strategist	1. Develop a comprehensive vulnerability management strategy, encompassing scanning, prioritization, remediation, and continuous monitoring. 2. Utilize threat intelligence to prioritize vulnerabilities based on their potential impact and relevance to the organization's assets.
Threat Hunting Enhancement	1. Augment threat hunting capabilities by integrating advanced analytics and threat intelligence feeds to proactively identify potential security threats. 2. Develop and document threat hunting methodologies, incorporating creative and unconventional approaches to uncover hidden threats. 3. Create playbooks that guide analysts through augmented threat hunting processes, ensuring consistent and effective security analysis.

Author(s)

Manish Kumar

Skills Network