Bridewell

Copilot for Security: Prompt Engineering

Unlock the full potential of Microsoft Copilot for Security by learning best-practice for prompt engineering. During this engagement, our consultants will teach you how to engineer the best prompts for Copilot that meet your specific security needs, improve reliability, and reduce bias.

Common Challenges

Prompting Techniques

Understand when zero-shot, few-shot, and chain-of-thought prompting is appropriate to achieve complex tasks and improve reliability.

Contextual Understanding and Specificity

Craft prompts that accurately reflect the technical nature of cyber security topics, ensuring Copilot understands and responds with domain-appropriate language.

Bias Mitigation

Recognise and reduce biases in prompts to ensure fair, unbiased responses from Copilot, whilst maintaining relevance and accuracy.

Response Interpretation

Effectively interpret Copilot's responses, especially when dealing with open-ended prompts.

How Bridewell Can Help

Prompt Masterclass

Our consultants demonstrate the most effective prompt mechanisms for different scenarios, ensuring systems respond accurately in different operational contexts.

Custom Prompt Development

Develop prompts for your specific security needs, operational context, and prompts for reporting.

Response Playbooks

Enhance your existing incident response playbooks, incorporating the use of Copilot to reduce the time to remediate.

Prompt Evaluation Services

Using our own prompt evaluation framework, we can review your existing prompts and evaluate their effectiveness.
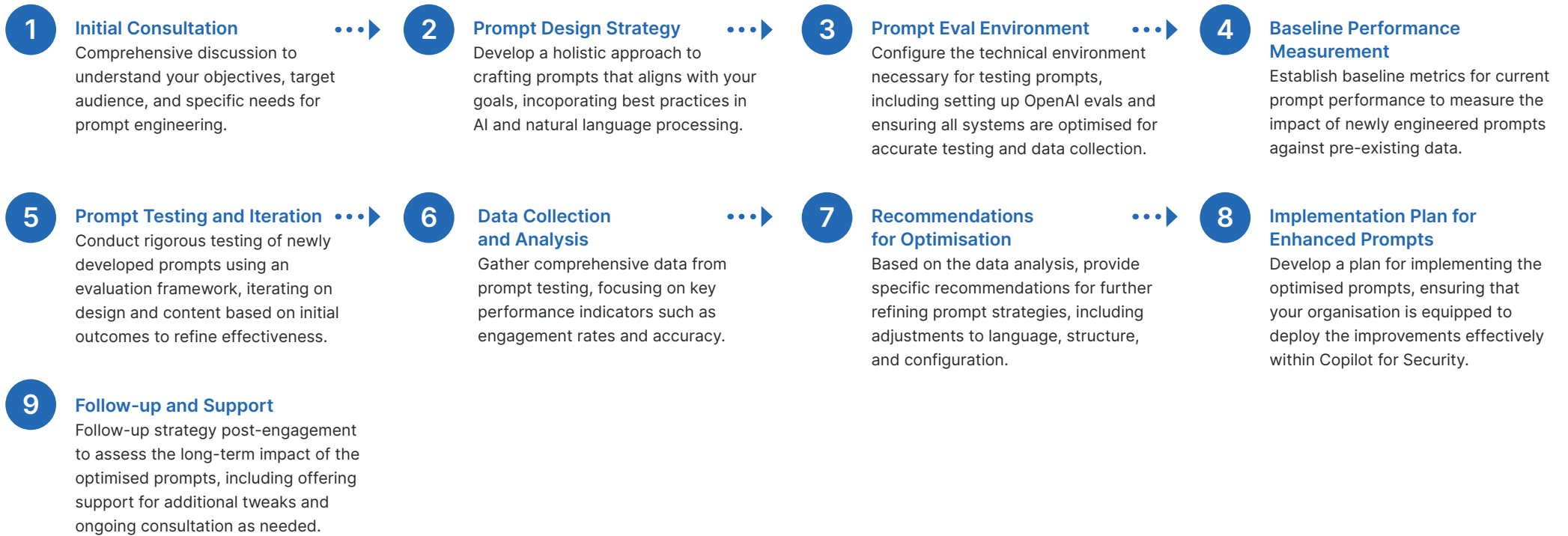
Improved Return on Investment

We provide guidance on effectively utilising Microsoft Copilot for Security to mature your security posture.

Schedule a Consultation With Our Team

Speak with our team for more insight on how you can leverage Copilot for Security.

Bridewell

Microsoft Intelligent
Security Association

Microsoft Security   Microsoft Verified
Managed XDR Solution

Microsoft
Solutions Partner
Security

Specialist
Cloud Security
Threat Protection

Copilot for Security: Prompt Engineering

1 Initial Consultation
Comprehensive discussion to understand your objectives, target audience, and specific needs for prompt engineering.

2 Prompt Design Strategy
Develop a holistic approach to crafting prompts that aligns with your goals, incoporating best practices in AI and natural language processing.

3 Prompt Eval Environment
Configure the technical environment necessary for testing prompts, including setting up OpenAI evals and ensuring all systems are optimised for accurate testing and data collection.

4 Baseline Performance Measurement
Establish baseline metrics for current prompt performance to measure the impact of newly engineered prompts against pre-existing data.

5 Prompt Testing and Iteration
Conduct rigorous testing of newly developed prompts using an evaluation framework, iterating on design and content based on initial outcomes to refine effectiveness.

6 Data Collection and Analysis
Gather comprehensive data from prompt testing, focusing on key performance indicators such as engagement rates and accuracy.

7 Recommendations for Optimisation
Based on the data analysis, provide specific recommendations for further refining prompt strategies, including adjustments to language, structure, and configuration.

8 Implementation Plan for Enhanced Prompts
Develop a plan for implementing the optimised prompts, ensuring that your organisation is equipped to deploy the improvements effectively within Copilot for Security.

9 Follow-up and Support
Follow-up strategy post-engagement to assess the long-term impact of the optimised prompts, including offering support for additional tweaks and ongoing consultation as needed.

About Bridewell

Bridewell specialises in protecting and transforming organisations operating in Critical National Infrastructure (CNI), as well as those who want the highest standard of security. Our team are highly accredited by major industry bodies and have extensive experience delivering cyber consulting and managed security services across multiple sectors. As a long-standing Microsoft partner, our team are also experts in maximising the effectiveness of Microsoft Security solutions.

We have a deep understanding of the challenges faced by CNI organisations and work in continuous partnership with our clients to find the right solutions to defend them from threats and attacks.

Get in Touch

📞 +44 (0)3303 110 940

✉ hello@bridewell.com

➤ bridewell.com

Assured Service Provider — In association with National Cyber Security Centre — Cyber Incident Exercising
Assured Service Provider — In association with National Cyber Security Centre — CHECK Penetration Testing
Assured Service Provider — In association with National Cyber Security Centre — Cyber Incident Response (Level 2)
Assured Service Provider — In association with National Cyber Security Centre — Consultancy: Audit & Review
Assured Service Provider — In association with National Cyber Security Centre — Consultancy: Risk Management
UK Civil Aviation Authority
ASSURE
AICPA SOC 2
CREST — VA PEN TEST CSIR SOC
CfA ISO 27001 UKAS
CfA ISO 9001 UKAS
Crown Commercial Service Supplier
PCI Security Standards Council
Ecologi — climate positive workforce
CYBER ESSENTIALS PLUS