**How AI Is Helping Cybersecurity Pros Work Smarter, Not Harder**

* AI can streamline daily work, letting you focus on high-impact tasks instead of repetitive ones.
* Luis, a Cloud Security Architect at Google, uses AI to:
  + Understand complex security frameworks.
  + Find bugs in code.
  + Create technical content.
  + Lead workshops and advocate for improvements in Google Cloud.

**Prompting Effectively with the T-C-R-E-I Framework**

1. **Task**
   * Define what you want the AI to do.
   * Include **persona** (e.g., a cybersecurity analyst) and **format** (e.g., bulleted list or paragraph).
2. **Context**
   * Provide details the AI needs (e.g., your role, your audience, constraints like budget or scope).
3. **References**
   * Add past examples or content for the AI to draw from (when available).
4. **Evaluate**
   * Assess whether the output meets your needs.
5. **Iterate**
   * Improve your prompt based on output quality.

**Tips for Better Prompts**

* Use complete sentences and natural language.
* Be specific and direct.
* It's okay to reorder or adjust the framework—substance matters more than sequence.

**Responsible AI Use in Cybersecurity**

* Use a **human-in-the-loop** approach: validate outputs with expert judgment.
* Always check organizational policies before using AI on sensitive data.
* Even outside of work, avoid entering confidential or personal information.

**Applicable Across Tools**

* Techniques shown with Gemini apply broadly to other Gen AI tools like ChatGPT, Copilot, and Claude.

**Final Thought**

* AI helps cybersecurity professionals shift from reactive, tedious tasks to strategic work where their skills make the biggest difference.

**Using AI to Understand Security Frameworks like NIST 800-53**

* **Security analysts** identify assets, assess risks, and apply controls based on chosen frameworks.
* **Security frameworks** (e.g., NIST 800-53) guide implementation of safeguards for data and privacy.
* These documents are often **dense and complex**, even for experienced professionals.

**Example: Control SI-5 from NIST 800-53 Rev. 5**

* SI-5 focuses on **Malicious Code Protection**, outlining how to detect, prevent, and respond to malware threats.
* Enhancements strengthen the control but are **not mandatory for non-federal systems**.
* AI tools like **Gemini** can explain:
  + What SI-5 is asking you to do.
  + How to implement it practically.
  + Which enhancements are **worth considering** for stronger security.

**Effective Prompting Example**

“I'm a security analyst and I need help understanding control SI-5 in NIST 800-53 rev 5. What does it ask me to do? How can I implement this control? And what enhancements should I consider adopting? I'm not developing a federal system, but would like high levels of security, so the enhancements are not requirements per se, though they are desirable.”

* This prompt works well because it provides:
  + **Clear task**
  + **Relevant context**
  + A **specific reference** (SI-5)
  + Clear explanation of your **security goals and system type**

**Tip: Customize How You Learn with Gen AI**

* Stuck? Ask for a different explanation style:
  + “Explain this like I’m new to cybersecurity.”
  + “Use a metaphor or real-world example.”
  + “Break it down like I’m in elementary school.”

**Bonus Tip: Use Voice Input**

* Tools like Gemini support **microphone input**—a quick way to:
  + Iterate prompts.
  + Add clarifications.
  + Make learning **interactive and fast**.

**Bottom Line**

* AI tools help make **long, technical documents like NIST 800-53** more digestible.
* Use them to **learn, clarify, and implement** controls more effectively—no need to struggle through it alone.