**Using Gen AI to Understand and Manage Security Vulnerabilities**

* Every asset has many potential vulnerabilities, and the volume of information about them can feel overwhelming.
* Gen AI tools like Gemini can help:
  + Explain the basics of vulnerabilities clearly and impartially.
  + Assess how critical a vulnerability is to your systems.
  + Suggest immediate mitigation steps, even before official patches are available.
* Example Prompt:
  + *"I am a junior cybersecurity analyst, new to the field. I've recently become aware of the following vulnerabilities: Server-side request forgery, injection, cryptographic failures, and broken access control. Define what each of these are, identify their potential impact, and provide suggestions for immediate mitigation steps."*
  + This includes *Context* (from the T-C-R-E-I framework) by stating your experience level, helping tailor the AI's response.
* Gemini’s Output:
  + Defines each vulnerability clearly.
  + Explains its potential impact on an organization.
  + Offers actionable mitigation suggestions.
  + Supports building foundational knowledge for new professionals.
* Evaluating and Iterating (E and I in T-C-R-E-I):
  + Assess whether the output fully meets your needs—are the mitigation steps detailed enough?
  + If not, iterate:
    - Ask for more detailed explanations.
    - Rephrase confusing sections.
    - Provide examples of preferred formats or styles.
    - Break instructions into shorter, clearer sentences.
    - Highlight what you liked or disliked in the output and request a refined response.
* Tips for Better Prompting:
  + Ensure your prompt has enough detail to guide the AI tool effectively.
  + Share example outputs when possible to clarify expectations.
  + Keep refining the prompt until the output aligns with your goals.
  + Keep asking “why” to uncover deeper insights about vulnerabilities and their causes.
* Responsible Use:
  + Always validate AI outputs against trusted sources.
  + Maintain a human-in-the-loop approach to avoid relying solely on AI for critical security information.
* Bonus Tip:
  + Preparing for interviews? Ask the AI tool for sample interview questions on vulnerabilities.
  + Practice your responses, then compare them to the AI’s to identify strengths and areas for improvement.

**Using Gen AI Tools for Detection and Incident Response**

* Detection and incident response are critical in cybersecurity.
* Security analysts monitor networks for anomalies and suspicious traffic.
* Alerts generated from anomalies require investigation by reviewing logs.
* Gen AI tools like Gemini can assist by:
  + Reviewing alert information.
  + Prioritizing threats based on severity and potential system impact.
* Example Prompt:
  + *"I've been tasked with addressing and resolving three intrusion detection system alerts about suspicious network activity. Review the alert information below and help me prioritize these threats based on severity and potential impact."*
  + Providing alert details gives context for a tailored AI response.
* Gemini’s Output:
  + Produces a prioritized list of alerts.
  + Explains reasoning behind each priority.
  + Highlights additional considerations such as:
    - Correlations between alerts (e.g., SYN flood as a possible diversion).
    - Importance of having a well-defined incident response plan.
* Incident Response Plan:
  + A documented set of procedures guiding each step during an incident.
  + Essential for quick, efficient, and effective response.
  + AI tools can help identify appropriate responses when incidents fall outside the documented plan.
  + AI can also assist in updating and documenting missing alert types or vulnerabilities in the plan.
* Tips for Using AI Tools in Incident Response:
  + Experiment with prompts to find what works best for you.
  + Treat learning AI as a journey—test, explore, and adapt.
  + Use AI to save time and gain insights on complex or unfamiliar tasks.
* Challenge:
  + Identify time-consuming tasks or projects where AI can make a real difference.
  + Commit to experimenting with AI to improve your cybersecurity work.