Explain It to Me Like I'm an Engineer! Using Chat GPT to Describe Security Controls to Everyone Who Isn't an ISSO

Greg Elin
Principal OSCAL Engineer
RegScale, Inc.

ChatGPT and the new Generative AI tools excel at summarizing and re-phrasing existing text. We can prompt these tools to provide us with information "in the style of X" or explain a concept us "like I'm a fifth grader." We can leverage this capability to translate jargon-filled, abstract security controls in the NIST SP 800-53 documents to meaningful information for specific roles and situations. Software developers, project managers, UX designers, ISSOs, system owners, enterprise architects, executives have different frames if reference and terminology through which they view information systems.

Wouldn't it be nice if NIST published a version of its controls, maybe all of it documents, rewritten for these specific audiences? Wouldn't it be nice if you could request an explanation of a term after hours?

This presentation will demonstrate how Generative AI makes this possible and how to incorporate this capability safely into our tools without the risk of exposing our vulnerabilities and overdue POA&Ms to giant black box regurgitation machines. Using ChatGPT and other cloud based LLM services to assist the entire team shimmy up the learning curve can do much to improve our cybersecurity compliance without the risk of leaking sensitive security information.