Concept1: Compliance Development Using AIML & GenAI

Background:

Prestigious organisations and Authorities like the Center for Internet Security (CIS), Defense Information Systems Agency (DISA), and PCI DSS publish compliance content that provides guidelines for securing and compliant systems. These documents are tailored for diverse operating system types or network devices and versions.

Within these documents lie the blueprints for rules and rule sets essential for crafting compliance content templates, complete with remediation strategies (May be only for some of the rules). The complexity and breadth of these documents demand thorough *scrutiny to avoid overlooking crucial rules, rendering the analysis process inherently time-intensive.*

Content development involves several key tasks: creating compliance detection scripts, developing configuration and remediation scripts, identifying rules that need fixing, designing user-friendly templates, and automating the generation of remediation scripts for noncompliant regulations to streamline the workflow.

In certain scenarios, the specificity of scripts, scripting languages, and deployable payloads align with the nuances of distinct operating systems. For instance, PowerShell or batch scripts cater to Windows environments. In contrast, shell scripts are tailored for Unix-based systems, ensuring precise and effective compliance management across diverse platforms or network devices.

The Compliance documents published by the authorities provide guidelines and rules, categorised into two primary action types: audit and remediation.

- ***Audit Action Type:*** *This involves assessing the current state of a system or network to determine compliance with established security standards. Audit scripts or commands are executed on endpoints to collect relevant information. For example, auditing scripts may query system configurations, check for specific file permissions, or examine network settings. In short, it's a script or series of commands that detect whether a system is compliant or not.*
- ***Remediation Action Type:*** *Once audit results identify non-compliant areas, remediation becomes imperative to mitigate security risks. Remediation scripts or commands are designed to correct identified issues and bring systems into compliance. These scripts typically automate tasks such as applying configuration changes, installing patches, or modifying access controls.*

Script Types and Platforms

The script type employed depends on the selected platform, with distinct approaches for Windows, Linux/Unix environments, and network devices.

a. ***Windows Platform***

        i. ***PowerShell**: PowerShell scripts are commonly used for audit and remediation actions on Windows systems. They offer robust automation capabilities and access to a wide range of system management functionalities.*
        ii. ***Series of Windows Native Commands**: In cases where PowerShell is not preferred or available, a series of native Windows commands can be utilised to achieve audit and remediation objectives.*
        iii. ***Batch Script***

    b. ***Linux/Unix Platform:***
        i. ***Shell Scripts**: Shell scripts are the primary choice for audit and remediation tasks on Linux/Unix systems. They offer flexibility and efficiency in executing commands and managing system configurations.*
        ii. ***Series of Linux/Unix Native Commands**: Like Windows, Linux/Unix environments can leverage native commands for audit and remediation, providing granular control over system elements.*

Problem Statement:

The IT team spends a good amount of time analyzing the PDF and XML documents published by CIS, DISA, and PCI authorities to generate audit and remediation scripts for the templates. Compliant Organizations are mandated and publish Compliance reports at regular intervals.

- *There is a huge list of operating systems and OS versions for which authorities publish and update the content on a regular basis.*
- *Authorities keep on publishing the updated content to keep up with the latest security guidelines.*
- *Due to their size and complexity, these documents require careful attention to detail, which makes the complete process time-consuming.*
- *When updated content is published, duplicate work/efforts need to be put in during this process for similar rules with small changes in their attributes.*

Expected solution/outcome and Eval Criteria:

The group must demo the working model and will be evaluated on the following.

1. *Groups will focus on CIS and DISA templates.*
2. *Groups are free to use any AI tools.*
3. *Module selection and structure: Choosing an appropriate machine learning model or algorithm that is suitable for the task at hand.*
4. *Data Extraction and Model training*
5. *Querying Model for Compliance Template version for Rules and Rule groups.*

6. *Automatic/On-Click Script Generation: For a specific template, version, rule, operating system, network devices, and Script Type.*
7. *Reliability, Robustness, Accuracy and Consistency of scripts*
8. *APIs exposed for the operations carried out as part of the solution.*
9. *UI Representation of process and operations.*
10. *Design and Architecture of solution.*
11. *Creativity*

Pre-Requites and Material:

Comprehensive compliance PDFs and XML files will be made available on the day of the briefing, ensuring participants have all necessary resources for an informed discussion.